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.

conventions sur la preuve (art. 1316-2 C. civ.), entérinant ainsi une jurisprudence constante [35].

Avec la signature numérique, l'émetteur du message peut être identifié au moyen d'un certificat de signature et l'intégrité du contenu du message pourra être vérifiée. L'identification électronique peut également s'effectuer au moyen de procédés biométriques (ex.: empreinte digitale ou iris de l'œil). Toutefois, comme pour les signatures numériques actuellement sur le marché, les prestataires de services et les industriels de la sécurité adjoignent à ces identifiants directement liés à la personne des certificats numériques d'identification.

La reconnaissance des effets juridiques des signatures électroniques figure à l'article 5 de la directive. Or, la signature électronique ne relève pas d'une approche de sécurité unique: sa sécurité est variable comme la reconnaissance de ses effets juridiques suivant le statut de la signature. L'article 2-2 établit les exigences de la « signature électronique avancée » (SEA): elle doit être liée uniquement au signataire et permettre de l'identifier, « être créée par des moyens que le signataire puisse garder sous son contrôle exclusif » et enfin, elle doit être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable (la fonction « abrégé » ou « contrôle » des signatures numériques permettant d'assurer l'intégrité). Les annexes III et IV précisent les dispositifs de création et de vérification de signature.

Aux termes de l'article 5 § 1, les États doivent veiller à ce que les signatures électroniques avancées basées sur un certificat qualifié (annexes I et II) et générées par un dispositif sécurisé de création de signature (annexe III) « a) 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; b) soient recevables comme preuves en justice ». *Les signatures électroniques qui répondent aux conditions de sécurité des SEA sont par conséquent juridiquement équivalentes aux signatures manuscrites.* L'assimilation doit être pleine et entière.

L'article 5 § 2, en revanche, s'applique aux autres signatures électroniques qui ne correspondent pas aux critères de la SEA et énonce un principe de non-discrimination à leur égard en ces termes: « Les États membres doivent veiller à ce que l'efficacité juridique et la recevabilité comme preuve en justice

35. Civ. 1re, 5 nov. 1952, *Bull. civ.* I, nº 286; Civ. 3e, 16 nov. 1977, *Bull. civ.* III, nº 393. Selon la doctrine « les parties peuvent écarter les exigences de l'article 1341, et convenir que la preuve des contrats qu'elles passeront ou qu'elles ont passés, se fera par d'autres modes que l'écrit. » H., L. et J. Mazeaud, F. Chabas, *Leçons de droit civil, Introduction générale*, Paris, Montchrestien, 1991, nº 401; J. Ghestin et G. Goubeaux, *Traité de droit civil, Introduction générale*, 3e éd., Paris, LGDJ, 1990, nº 567.

ne soient pas refusées au seul motif que la signature se présente sous une forme électronique ou qu'elle ne repose pas sur un certificat qualifié, ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature ». *L'utilisation de ces procédés de signatures électroniques implique que l'on démontre, devant le juge, leur fiabilité technique.* Sous cette réserve ou dans le cadre d'une convention sur la preuve, leur valeur juridique est équivalente à celle des SEA.

Selon l'*European Electronic Signature Standardization Initiative* (EESSI) [36], l'article 5 de la directive laisserait apparaître deux niveaux de signatures :

- les signatures électroniques auxquelles on ne peut dénier les effets juridiques, ce qui pourrait avoir pour conséquence de voir reconnaître une simple signature réalisée au moyen d'un « scanner », donc reproductible indéfiniment sans aucune garantie qu'elle émane de la personne et que cette dernière manifeste son adhésion à l'acte qu'elle est censée signer [37] ;

- les signatures qui remplissent des exigences techniques et qui possèdent une valeur juridique identique à celle accordée aux signatures manuscrites (les signatures électroniques avancées).

En outre, si le cadre communautaire consiste à définir une base minimale d'harmonisation, il risque toutefois d'engendrer des niveaux de sécurité disparates, variables selon les États membres. Nous verrons cependant que les pouvoirs conférés à la Commission devraient permettre de remédier à cette disparité, une fois que le marché de la certification aura pris son essor.

Ainsi, toute méthode ou procédé technologique qui permet de réaliser les fonctions juridiques d'identification de l'auteur et d'approbation du contenu de l'acte, avec un degré suffisant de fiabilité sera reconnu comme remplissant les exigences d'une signature qui pourrait figurer dans une loi, si le juge la considère comme étant fiable. Dans le système juridique français, la SEA n'est pas mentionnée, un autre terme est utilisé : la signature électronique sécurisée.

---

36. L'EESSI est un organisme de normalisation.

37. De telles « signatures » n'apportent aucune garantie intrinsèque quant à la manifestation du consentement de la personne ; en effet, elles peuvent être produites par n'importe quelle personne (y compris le véritable signataire). Ce type de marque n'est qu'une copie et ne devrait être admis que sous certaines conditions, au risque de dévaluer la confiance que l'on accorde aux signatures électroniques véritablement fiables.

B. - *Le cadre français* [38]

Dans le prolongement des développements jurisprudentiels et doctrinaux, la loi du 13 mars 2000 a donné pour la première fois une définition légale en suivant une approche fonctionnelle de la signature. Ainsi, selon l'article 1316-4 alinéa 1er du Code civil, la signature (qu'elle soit électronique ou manuscrite) doit remplir 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 générale de la signature électronique se retrouve à l'article 1316-4, alinéa 2 du Code civil 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'État ». 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. À l'heure actuelle, seules les signatures électroniques basées sur la cryptologie à clé publique (à savoir les signatures numériques) répondent *a priori* à ces exigences légales et notamment à la garantie de la solidité du lien logique entre la signature et le message. Par conséquent, seule la signature numérique pourra être considérée comme une signature électronique sécurisée.

Celle-ci se définit suivant l'article 1.2 du décret du 30 mars 2001 [39] comme: « une signature électronique qui satisfait, en outre, aux exigences suivantes:

- être propre au signataire;

- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;

- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ».

Cette signature électronique sécurisée est présumée fiable, contrairement aux autres types de signature dont la fiabilité devra être démontrée, si elle est « établie grâce à un dispositif sécurisé de création de signature électronique

38. V., É. A. Caprioli, « Commentaires du décret nº 2001-272 du 30 mars 2001 relatif à la signature électronique », *RD banc. fin.* 2001. 3. 155; L. Jacques, « Le décret nº 2001-272 du 30 mars 2001 relatif à la signature électronique », *JCP* 2001. Aperçu rapide. 1601; F. Coupez et C. Gailliègue, « Vers une signature électronique juridiquement maîtrisée. À propos de l'arrêté du 31 mai 2002 », *CCE* nov. 2002. 8 s.

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

et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié » [40].

Au vu de cette définition doivent donc être pris en compte le dispositif sécurisé de création de signature électronique et le certificat électronique qualifié [41] pour caractériser une signature électronique sécurisée. Or, comme l'énonce l'article 6 du décret du 30 mars 2001, « Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II ». Ces dispositions s'appliquent également en matière de validité juridique de l'acte en vertu du nouvel article 1108-1 du Code civil introduit par la LCEN. Pour que la présomption de fiabilité joue pleinement, le PSCE devra procéder à une demande d'accréditation auprès des organismes compétents.

D'une point de vue strictement juridique, peu importe que la signature soit sécurisée, qu'elle utilise un certificat qualifié ou au contraire qu'elle soit simple ; elles ont toutes la même valeur juridique. C'est au juge qu'il appartient de décider de l'admissibilité et de la valeur juridique de la preuve électronique qui lui est soumise. Pour les signatures électroniques simples, ce qui englobe toutes les signatures électroniques ne bénéficiant pas de la présomption de fiabilité, c'est à l'utilisateur du procédé de rapporter la preuve de sa fiabilité. Pour les signatures électroniques sécurisées (bénéficiant de la présomption de fiabilité), c'est à la personne qui conteste la fiabilité d'en rapporter la preuve.

---

40. Art. 2 Décr. 30 mars 2001.

41. Ce certificat d'identification délivrée par le PSCE devra pour être considéré comme qualifié, comporter :

« a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;

b) L'identité du prestataire de services de certification électronique ainsi que l'État dans lequel il est établi ;

c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;

d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

f) L'indication du début et de la fin de la période de validité du certificat électronique ;

g) Le code d'identité du certificat électronique ;

h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;

i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé ».

II. - Le schéma français d'accréditation des prestataires de services de certification

L'article 3 de la directive 1999/93 dispose :

« 1. Les États membres ne soumettent la fourniture des services de certification à aucune autorisation préalable.

2. Sans préjudice des dispositions du paragraphe 1, les États membres peuvent instaurer ou maintenir des régimes volontaires d'accréditation visant à améliorer le niveau du service de certification fourni. Tous les critères relatifs à ces régimes doivent être objectifs, transparents, proportionnés et non discriminatoires. Les États membres ne peuvent limiter le nombre de prestataires accrédités de service de certification pour des motifs relevant du champ d'application de la présente directive.

3. Chaque État membre veille à instaurer un système adéquat permettant de contrôler les prestataires de service de certification établis sur son territoire et délivrant des certificats qualifiés au public.

4. La conformité des dispositifs sécurisés de création de signature aux conditions posées à l'annexe III est déterminée par les organismes compétents, publics ou privés, désignés par les États membres. La Commission, suivant la procédure visée à l'article 9, énonce les critères auxquels les États membres doivent se référer pour déterminer si un organisme peut être désigné.

La conformité aux exigences de l'annexe III qui a été établie par les organismes visés au premier alinéa est reconnue par l'ensemble des États membres.

5. Conformément à la procédure visée à l'article 9, la Commission peut attribuer, et publier au Journal officiel des Communautés européennes des numéros de référence de normes généralement admises pour des produits de signature électronique. Lorsqu'un produit de signature électronique est conforme à ces normes, les États membres présument qu'il satisfait aux exigences visées à l'annexe II, point f), et à l'annexe III.

6. Les États membres et la Commission œuvrent ensemble pour promouvoir la mise au point et l'utilisation de dispositifs de vérification de signature, à la lumière des recommandations formulées, pour les vérifications sécurisées de signature, à l'annexe IV et dans l'intérêt du consommateur [...] ».

Ce régime volontaire d'accréditation a été transposé dans différents États de l'Union européenne. Notre analyse se bornera à étudier le dispositif français.

En France, les principes du schéma d'accréditation des PSCE découlent directement de la directive et de ses annexes. En application de ces règles, deux types d'organismes ayant des attributions différentes doivent interve-

nir. Les premiers, issus du décret du 18 avril 2002, sont chargés de l'évaluation et de la certification des produits et systèmes des technologies de l'information (B), tandis que les seconds, revisités par l'arrêté du 26 juillet 2004, seront impliqués dans la reconnaissance de la qualification des PSCE et l'accréditation des organismes chargés de l'évaluation (A). Rappelons toutefois que la procédure générale d'évaluation et de certification ne concerne que l'aspect administratif de la démarche ; l'aspect technique étant précisé dans des documents normatifs. Ainsi, pour les produits de signatures électroniques conformes aux exigences des annexes II f) et III de la directive, les normes ont été publiées au *Journal officiel des Communautés européennes* [42].

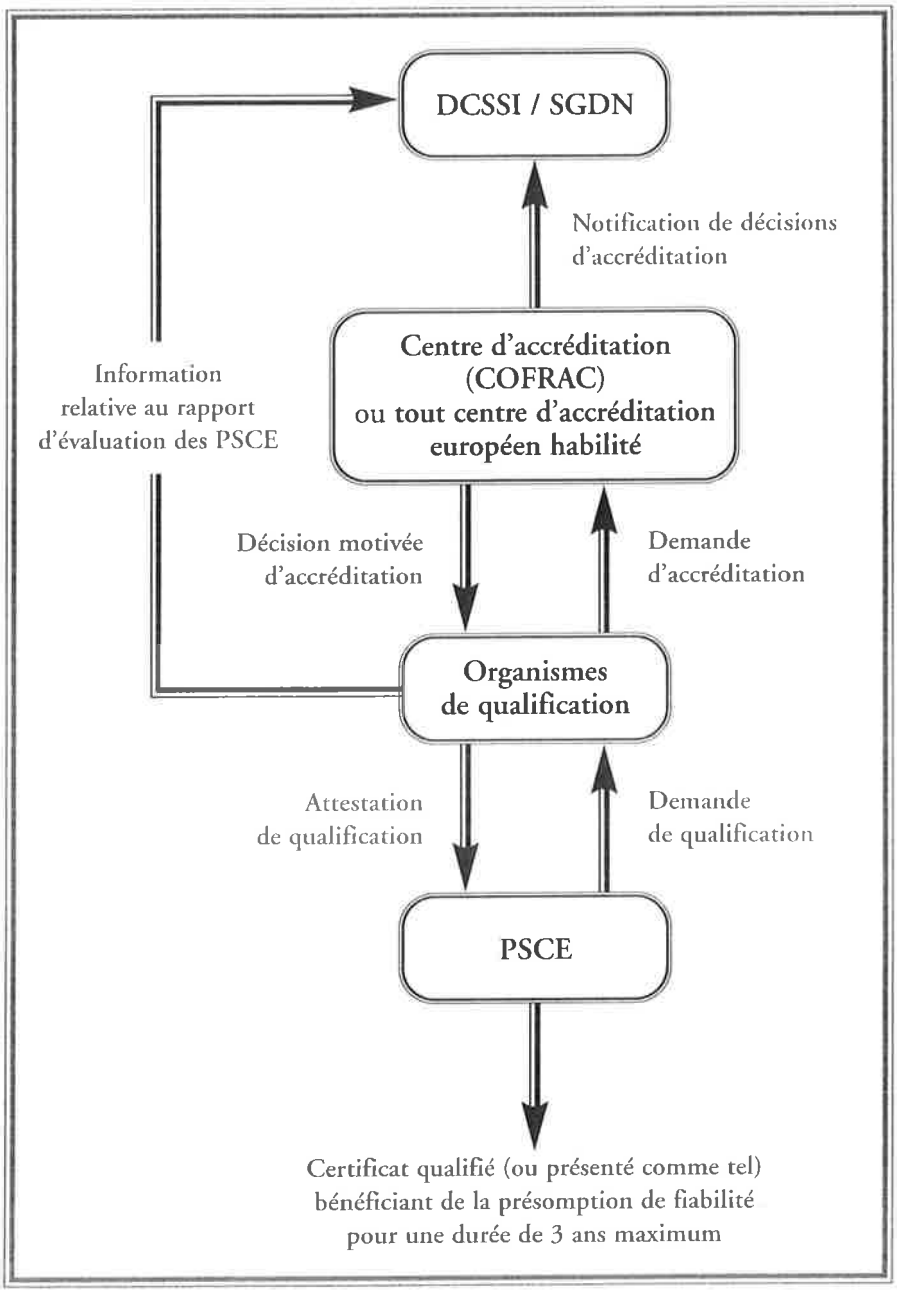
A. - *La procédure de qualification du PSCE*

À titre liminaire, il convient de préciser que la notion de « qualification » en droit français correspond à la notion d'« accréditation » en droit communautaire. De manière simplifiée, retenons qu'un organisme accrédité suivant des conditions particulières par une autorité nationale (en France, le COFRAC) ou étrangère pourra effectuer une procédure de qualification pour un PSCE donné. Ainsi, un titulaire de certificat présenté comme qualifié pourra s'assurer de la fiabilité des pratiques d'un PSCE. En effet, un PSCE qualifié sera présumé fiable et, par voie de conséquence, le certificat qu'il délivrera comme étant qualifié sera également présumé fiable.

L'arrêté du 26 juillet 2004 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 met en place une procédure comportant un double niveau : l'accréditation des organismes d'évaluation des PSCE et la reconnaissance de la qualification de ces derniers.

42. Décis. Commission 14 juill. 2003, nº 2003/511, relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques, conformément à la directive 1999/93/CE du Parlement européen et du Conseil, *JOCE* 15 juill. 2003, L. 175, p. 45 s.

DISPOSITIF MIS EN PLACE EN FRANCE EN MATIÈRE DE QUALIFICATION DE PSCE



Les organismes qui procèdent à l'évaluation des PSCE sont accrédités par des centres à l'issue d'une procédure. On les appelle « organismes de qualification ». Il convient de préciser qu'en France cette mission d'accréditation sera remplie par le Comité français d'accréditation (COFRAC), reconnu par l'arrêté du 30 mars 1995 [43] en tant qu'instance d'accréditation des organismes certificateurs de produits industriels et de services. En outre, tout centre d'accréditation signataire de l'accord multilatéral de reconnaissance mutuelle pris dans le cadre de la coopération européenne des organismes d'accréditation pourra être compétent. Les décisions motivées de ces centres d'accréditation doivent être communiquées à la Direction centrale de la sécurité des systèmes d'information (DCSSI).

Les demandes d'accréditation doivent répondre à un certain nombre d'exigences concernant l'identification de l'organisme demandeur ainsi que son activité d'évaluation des PSCE [44]. Pour respecter l'impartialité et l'indépendance nécessaires à une demande de qualification, l'organisme demandeur devra signaler au centre d'accréditation les liens éventuels qu'il entretient avec certains PSCE ainsi que les mesures qu'il compte mettre en place pour éviter tout conflit d'intérêt.

La demande examinée par le centre d'accréditation fera l'objet d'une décision motivée qui devra être notifiée à l'organisme demandeur et à la DCSSI. L'accréditation de l'organisme peut être accordée pour une période de cinq ans maximum. La conformité des organismes accrédités fera également l'objet de vérifications tout au long de leur activité de manière directe, à travers les vérifications effectuées par les centres, ou de manière indirecte, au moyen d'informations communiquées par ces organismes. En cas de non-conformité, l'accréditation pourra être retirée ou suspendue. Le centre d'accréditation mettra à la disposition du public la liste des organismes qu'il a accrédités.

Seul un organisme dûment accrédité pourra effectuer une procédure de qualification d'un PSCE. Cette procédure vise à évaluer les services proposés par les PSCE et plus particulièrement, la conformité des services proposés avec les spécifications techniques précisant les exigences de l'article 6 du décret du 30 mars 2001. Il est important de souligner que l'arrêté laisse libre choix aux PSCE quant aux éléments à présenter en vue de l'évaluation, ce qui pourrait être une faille dans le système visant l'établissement de la confiance.

À la fin de l'évaluation, une attestation délivrée par l'organisme accrédité comportera une description des services proposés par le PSCE, couverts par la qualification ainsi que la durée qui devra être inférieure à trois ans. L'attestation de qualification délivrée à un PSCE porte sur l'ensemble des services pour les certificats qualifiés ; elle ne doit pas être confondue avec l'attestation

43. *JO* 5 avr., p. 5439 s.
44. Art. 2 Arr. 26 juill. 2004.

de conformité qui sera délivrée à un opérateur technique (opérateur de services de certification), lequel peut travailler pour un ou plusieurs PSCE.

Les PSCE qualifiés devront faire appel à des produits et systèmes informatiques certifiés (modules cryptographiques) pour produire des certificats reconnus comme qualifiés.

B. - *La certification des produits et systèmes des technologies de l'information*

Le décret nº 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information [45] a mis en place un système de certification nécessaire à la délivrance de signatures électroniques sécurisées. Cette certification doit s'appliquer aux dispositifs de création de signature. En effet, pour disposer d'une signature électronique considérée comme sécurisée, il faut non seulement que le titulaire bénéficie d'un certificat qualifié mais aussi d'un dispositif de création reconnu comme sécurisé, c'est-à-dire répondant aux exigences du décret nº 2002-535. Une multitude d'organismes intervient dans ce système : le Comité directeur de la certification en sécurité des technologies de l'information [46], la DCSSI et les centres d'évaluation des produits et systèmes.

L'article 4 du décret du 30 mars 2001 crée un « Comité directeur de la certification en sécurité des technologies de l'information » en tant qu'organisme régulateur du système. Présidé par le secrétaire général de la défense nationale ou son représentant, il rend compte de ses travaux au Premier ministre et la DCSSI en assure le secrétariat. Cette dernière est d'ailleurs chargée d'organiser la procédure d'agrément des centres d'évaluation et d'évaluer leur activité.

Les centres d'évaluation sont ainsi soumis à une procédure d'agrément, déclenchée par le dépôt d'une demande précisant le domaine dans lequel l'organisme entend exercer son activité. Le demandeur devra ainsi apporter la preuve d'un certain nombre d'éléments : sa conformité aux critères de qualité selon les règles et normes d'accréditation en vigueur, son aptitude à appliquer les critères d'évaluation en vigueur et la méthodologie correspondante. Il

---

45. *JO* 19 avr., p. 6944. V., A. Penneau, « La certification des produits et systèmes permettant la réalisation des actes et signatures électroniques (à propos du décret nº 2002-535 du 18 avril 2002) », *D.* 2002. Chron. 2065 ; *Dr. et patr.* févr. 2003. 116, obs. É. A. Caprioli.

46. V. concernant les membres de ce comité, Arr. 28 févr. 2003 portant nomination au comité directeur de la certification en sécurité des technologies de l'information, *JO* 2 mars, p. 3743.

devra également assurer la confidentialité requise par l'évaluation et leur compétence technique à conduire une évaluation appréciée par la DCSSI.

L'organisme fera l'objet d'une évaluation par la DCSSI qui prendra en compte la compétence technique du demandeur. Celui-ci devrait également présenter une accréditation délivrée par une instance reconnue dans les conditions prévues à l'article R. 115-6 du Code de la consommation [47], ou encore délivrée par une instance étrangère. À la suite de cette étape, le Comité directeur donnera son avis en vue de l'obtention de l'agrément qui est accordé par le Premier ministre pour une période de deux ans renouvelables. Il convient de souligner que l'agrément peut être limité à un niveau d'assurance déterminé [48].

Le contrôle de la DCSSI s'exerce également après la délivrance de l'agrément en vue de constater la conformité des centres d'évaluation aux critères déterminés lors de l'agrément [49].

La dimension européenne est envisagée par le décret par la mise en place d'un système de reconnaissance des agréments délivrés par des autorités situées à l'intérieur ou à l'extérieur de la Communauté européenne [50].

Les organismes ainsi agréés pourront procéder à l'évaluation des produits et systèmes des technologies de l'information. La personne, appelée le commanditaire, intéressée par une certification d'un produit ou d'un système devra déposer un dossier auprès de la DCSSI. Après avis positif de cette dernière, le commanditaire pourra choisir un des centres d'évaluation agréés qui remettra à la DCSSI un rapport d'évaluation servant de base pour l'élaboration d'un rapport de certification. Le certificat qui est délivré par le Premier ministre apporte une double attestation de conformité : du produit ou du système soumis à l'évaluation aux caractéristiques de sécurité spécifiées et de la procédure d'évaluation avec les règles et normes en vigueur [51].

Afin d'assurer l'efficacité du système dans une optique internationale, la DCSSI pourra passer, après avis du Comité directeur de la certification, des accords de reconnaissance mutuelle avec des organismes étrangers homologues. La reconnaissance pourra être limitée à un niveau d'assurance déterminé. Dans le cadre de cette certification de la sécurité de produits ou du

47. Aux termes de cet article : « l'impartialité et la compétence d'un organisme certificateur peuvent être établies par un document délivré à cet effet par une instance d'accréditation, reconnue par arrêté conjoint du ministre chargé de la consommation et du ministre chargé de l'industrie. Dans ce cas, le dossier accompagnant la déclaration prévue à l'article R. 115-1 ci-dessus peut ne comporter que les éléments cités aux 1, 2 et 3 de l'article R. 115-2 ». Il s'agit actuellement du COFRAC.

48. Art. 13 Décr.

49. Art. 14 Décr.

50. Art. 13 Décr.

51. Art. 8 Décr.

système de technologie de l'information, les certificats étrangers délivrés dans des conditions équivalentes se voient accorder la même valeur juridique que les certificats français [52].

III. - Obligations et responsabilités des prestataires de services de certification

Les PSC (PSCE en droit français) délivrent, à titre principal, des certificats électroniques permettant d'établir le lien entre les données de vérification de signature électronique (clé publique) et le signataire [53].

Ces derniers devront non seulement répondre à des exigences juridiques mais également à des exigences techniques. Si les exigences juridiques sont énoncées dans le cadre juridique susmentionné, les exigences techniques se retrouvent, en majeure partie, dans des travaux internationaux réalisés à l'*Internet Engineering Task Force* (IETF) et à *l'European Telecommunications Standards Institute* (ETSI). Ce processus de normalisation permet la régulation de l'activité de PSCE en tentant d'assurer une interopérabilité technique minimale entre les différents prestataires. Dans cette optique technique, les différents PSCE se situent au cœur d'une infrastructure à clé publique (ICP) donnée [54]. Cette ICP comprend plusieurs entités qui ont des fonctions et des responsabilités distinctes. Plusieurs métiers coexistent : autorité de certification (le PSCE), opérateur de certification, autorité d'enregistrement, services de publication (annuaire ou liste de révocation des certificats ou des autorités de certification reconnues), autorité de validation (de signature ou de certificat), autorité de gestion de preuve. Il ressort de ce système que la confiance dépend de l'ensemble des composantes de l'ICP. Les PSCE au sein d'ICP auront intérêt, pour démontrer leur fiabilité technique et assurer cette interopérabilité, de respecter les dispositions de différents documents : une ou plusieurs politiques de certification (PC) ainsi qu'une ou plusieurs *déclaration des pratiques de certification* (DPC) ou « *certification practices statement* » (CPS).

Les PSCE jouent ainsi un rôle essentiel dans l'établissement de la confiance dans le cadre du commerce électronique. À ce titre, un certain nombre d'obligations pèsent sur le prestataire (A) qui pourra être tenu responsable vis à vis de ses clients et des personnes qui se fient à la signature électronique (B).

---

52. Art. 9 Décr.
53. Art. 1.11 Décr. 30 mars 2001.
54. Ou encore appelée infrastructure de gestion de clés (IGC).

A. - *Obligations du PSC*

Le système juridique français précise les obligations juridiques qui pèsent sur les PSCE qualifiés dans le cadre du décret du 30 mars 2001. Or, ces obligations sont la transposition quasi identique des annexes de la directive du 13 décembre 1999. La distinction entre les deux régimes (communautaire et français) ne se justifiant pas ici, seront examinées tour à tour l'émission de certificats qualifiés (1°) et les obligations du PSC au regard de la directive du 13 décembre 1999 (2°).

1° Émission de certificats qualifiés

Pour émettre des « certificats qualifiés », les « prestataires de services de certification » doivent fournir un certain nombre de garanties dont les exigences sont prévues à l'annexe II de la directive. Peu importe que le PSC bénéficie d'une accréditation volontaire ou qu'il se conforme à la directive sans passer par le régime d'accréditation. Sans entrer dans le détail des prescriptions de l'annexe II, nous signalerons que le PSC doit utiliser des systèmes et produits fiables tant pour leur fonctionnement que pour la conservation des certificats (annexe II, f et l) et employer du personnel qualifié (annexe II, e).

En cas de litige, ils auront également à faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification (annexe II, a). Les PSC doivent disposer des garanties financières suffisantes pour fonctionner en permettant l'indemnisation des utilisateurs autant que de besoin et notamment par le biais de la souscription d'une police d'assurance appropriée. S'agissant de la communication et de la reconnaissance avec d'autres PSC, il conviendra que l'interopérabilité des systèmes de signatures électroniques soit garantie, par exemple en respectant les normes et les standards en vigueur. Pour que toutes les parties intéressées aux services de certification (ex. : les abonnés, les tierces parties au contrat d'abonnement qui se fient aux certificats) puissent être en mesure de les utiliser dans leurs opérations en ligne, il est nécessaire que le PSC leur procure une information correcte « par un moyen de communication durable » sur l'ensemble des services qu'il propose et dans une langue compréhensible (en principe, au moins trois langues communautaires) (annexe II, k). Cette information doit être faite par écrit (elle peut être transmise par voie électronique) et doit également porter sur les termes et conditions contractuels, spécialement les procédures de réclamations et de règlement des litiges. L'existence d'un régime d'accréditation volontaire doit figurer sur le site. De la sorte, à notre avis, les personnes qui demandent un certificat seront informées de la situation du PSC (titulaire ou non de l'accréditation).

Lorsque le PSC fournit à son client des services de gestion de clés, il ne doit ni stocker, ni copier les données afférentes à la création de signature de celui-ci (annexe II, j). D'une part, cette exigence découle directement d'un principe de sécurité en vertu duquel il faut disposer de deux paires de clés distinctes lorsque l'on entend signer et chiffrer des messages. L'usage d'une seule paire de clés à la fois pour la signature et pour le chiffrement des messages aurait pour conséquence de créer le risque de voir un tiers s'approprier ou reconstituer la clé privée de signature d'une personne et qu'elle se fasse passer pour elle (usurpation d'identité). D'autre part, dans le cas de signature numérique, la clé privée doit rester secrète et sous le « contrôle exclusif » du signataire. Pour les clés de confidentialité, en revanche, le PSC peut être amené à les conserver dans l'hypothèse où un client, suite à la perte de sa clé, demanderait au PSC de la reconstituer (service de recouvrement de clé de confidentialité) pour être en mesure d'accéder à l'ensemble des fichiers qu'il aurait antérieurement chiffrés.

Dans toute ICP, l'enregistrement des abonnés aux services de certification s'effectue par l'entremise d'autorités d'enregistrement (AE). L'enregistrement peut s'effectuer soit en ligne et les pièces justificatives de l'identité sont envoyées par voie postale (pièces d'identité, extrait K-*bis*, et autres quittances attestant du domicile), soit de visu aux guichets prévus à cet effet (sur présentation des pièces justificatives). Cette opération est très importante car elle permet de vérifier l'identité conformément au droit national (annexe II, d), la capacité et les pouvoirs des personnes, de manière « à enregistrer toutes les informations pertinentes concernant un certificat qualifié » (annexe II, i). Cette entité ne souscrit pas d'engagement juridique envers les clients, elle est uniquement en relation contractuelle avec l'autorité de certification (AC). Cette dernière génère le certificat numérique d'identification sous sa seule responsabilité et à ce titre elle s'engage à remplir certaines obligations essentielles (art. 6 § 1 et § 2), c'est-à-dire établir et garantir le lien qui existe entre une personne et une paire de clés asymétriques dont elle est titulaire. En outre, le PSC crée et assure, sous sa responsabilité, le fonctionnement d'un service d'annuaire (rapide et sûr) et d'un service de révocation des certificats (fiable et immédiat) (annexe II, b).

2° **Obligations du PSC**

Il convient de signaler que les dispositions de la directive 93/13/CEE du Conseil du 5 avril 1993 relative aux clauses abusives dans les contrats conclus avec les consommateurs s'appliquent aux relations entre les PSC et les « abonnés » (article 3 § 5).

Aux termes de l'article 8 de la directive, les États membres doivent veiller à ce que les PSC et les organismes responsables de l'accréditation et du contrôle honorent les exigences posées par la directive 95/46/CE du Parle-

ment européen et du Conseil du 24 octobre 1995 relative au traitement des données à caractère personnel. À ce titre, l'article 5 de la loi nº 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel modifie la loi nº 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés en intégrant un article 33 qui dispose « sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par le prestataire de services de certification électronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures électroniques doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies » [55].

La directive prévoit des règles de responsabilité pour les PSC notamment eu égard au contenu des certificats (art. 6). En cas de préjudice, le PSC doit être responsable de l'exactitude des informations qu'il inscrit dans le certificat au moment de sa date d'émission, du lien entre le signataire et un bi-clé et enfin, de toute omission d'enregistrement et de publication de la révocation du certificat sur ses listes accessibles en ligne. Concernant l'exactitude des informations que le certificat doit contenir, il faut reconnaître qu'elles ne peuvent que résulter des pièces fournies lors de l'enregistrement (ex. : pièce d'identité, quittance). En cas de falsification, tant matérielle qu'intellectuelle, du ou des document(s), ou d'informations obsolètes, le PSC ne devrait pas être responsable des informations inscrites dans le certificat. En effet, actuellement les enregistrements s'effectuent le plus souvent en ligne et par l'envoi des pièces justificatives par courrier. Mais ce problème de faux documents serait le même dans le cadre des procédures d'enregistrement en face à face. Le PSC ne peut garantir que l'exactitude formelle des informations au vu des pièces transmises et non leur exactitude sur le fond. Dès lors, sa responsabilité ne peut être liée qu'à l'exacte transcription dans le certificat des informations fournies par l'abonné. Le titulaire du certificat devra, par conséquent, communiquer au PSC tous les changements affectant les informations contenues dans le certificat. Le PSC aura de la sorte la possibilité d'établir toute inexactitude et être dégagé, le cas échéant, de sa responsabilité.

En outre, « puisqu'une obligation d'exactitude pèse sur le prestataire à ce moment précis [la date de délivrance, art. 6 § 1, a], il [le PSC] doit veiller à ce que la date et l'heure d'émission puissent être déterminées avec précision [annexe II, b de la directive] ». Cette disposition suppose que des services d'horodatage soient opérationnels afin de garantir la fiabilité de la datation [56].

---

55. V., É. A. Caprioli, « Loi du 6 août 2004 : commerce à distance sur Internet et protection des données à caractère personnel », *CCE* 2005. 2. 24-28.

56. V. Ord. nº 2005-674, 16 juin 2005, relative à l'accomplissement de certaines formalités contractuelles par voie électronique (*JO* 17 juin, p. 10342 s.). Les art. 1369-7 et 1369-8 C. civ. relatifs aux lettres simples et recommandées électroniques prévoient que les exigences relative au procédé fiable de datation électronique seront précisées par décret.

S'agissant à présent de la personne physique ou morale ou de l'entité qui se fie *raisonnablement* au certificat (ou qui s'en prévaut) (art. 6 § 1 et § 2), il faut comprendre que le tiers doit vérifier non seulement la validité du certificat mais aussi celle de la signature. Dans cette perspective, une partie qui se fierait à un certificat sans consulter notamment la Liste de révocation des certificats (annuaire publié en ligne) ou les restrictions d'usage ou les valeurs limites contenues dans le certificat n'aura pas le droit d'engager la responsabilité du PSC. La validité du certificat et de la signature électroniques peut être attestée par une autorité de gestion de preuve.

B. - *Responsabilité du PSC*

La responsabilité est un élément majeur de la confiance qui doit être décliné au niveau européen et au niveau français.

1° Le cadre européen

Selon l'article 6 § 3 « Les États membres veillent à ce qu'un prestataire de services de certification puisse indiquer, dans un certificat qualifié, les limites fixées à son utilisation, à condition que ces limites soient discernables par des tiers. Le prestataire de services de certification ne doit pas être tenu responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation » et selon l'article 6 § 4 « dans un certificat qualifié, la valeur limite des transactions pour lesquelles le certificat peut être utilisé, à condition que cette limite soit discernable par des tiers. Le prestataire de services de certification n'est pas responsable des dommages qui résultent du dépassement de cette limite maximale. » Le terme « discernable » utilisé dans ces deux paragraphes peut surprendre le juriste, voire le laisser perplexe. Il signifie que les limites d'utilisation (ex. : engageant l'entreprise à l'exclusion de son employé en son nom personnel) du certificat doivent être perçues de façon à éviter toute confusion. Ainsi, il suffira que l'attention de la personne qui reçoit un certificat et un message signé soit attirée par une indication selon laquelle l'utilisation du certificat est limitée, sans qu'il soit nécessaire que ce soit tout le contenu de cette limite lui-même qui soit affiché. Ensuite (art. 6, § 4), les États devront exclure toute responsabilité du prestataire qui pourrait survenir à la suite d'une utilisation du certificat au-delà de la valeur limite des transactions (montants maximum) établie selon le certificat. Ces deux paragraphes doivent s'entendre comme étant une exclusion de tous les préjudices tant directs qu'indirects.

2° Le cadre français

L'article 33 de la LCEN qui transpose l'article 6 de la directive européenne du 13 décembre 1999 et par là la présomption de responsabilité pour les PSCE qui délivrent des certificats présentés comme qualifiés apporte quelques modifications qui se retrouvent notamment dans le régime de responsabilité du PSCE. Ainsi, lorsqu'il entend délivrer un certificat qualifié, le PSCE ne pourra pas exonérer sa responsabilité [57] en cas d'inexécution ou de mauvaise exécution d'une obligation de résultat.

De la sorte, cet article prévoit :

> « Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans des conditions fixées par décret en Conseil d'État lorsque :
>
> 1° Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;
>
> 2° Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;
>
> 3° La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;
>
> 4° Les prestataires n'ont pas fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers ».

Par conséquent, pour les certificats présentés comme qualifiés par le PSCE, le lien de causalité est présumé entre la faute (l'inexécution d'une obligation essentielle) et le préjudice (un manque à gagner pour le tiers qui se fie ou le signataire), sauf à démontrer qu'il n'a commis aucune faute intentionnelle ou qu'il n'a pas été négligent. Il en va de même pour les PSCE qui ont fait l'objet d'une qualification volontaire. La seule différence se situe dans la difficulté technique pour le demandeur de démontrer la faute commise par un PSCE qualifié.

Selon ce même article 33, « les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux

---

57. Pour de plus amples renseignements sur la responsabilité de plein droit, v. Ph. le Tourneau, *Droit de la responsabilité et des contrats 2004/2005*, Dalloz, coll. « Dalloz Action », 2004.

utilisateurs. » Le terme « *accessible* » pourrait être interprété en mettant en avant le fait que les limites d'utilisation du certificat doivent être perçues de façon à éviter toute confusion. En pratique, il pourrait s'agir d'une indication permettant à la personne qui reçoit un certificat et un message signé de remarquer les limites d'utilisation du certificat, sans qu'il soit nécessaire que ce soit tout le contenu de cette limite lui-même qui soit affiché. En effet, le tiers qui se fie (le destinataire du message signé) au certificat n'étant pas partie à la relation contractuelle nouée entre l'expéditeur et le PSCE, doit bénéficier de ces garanties et pour faire face à un éventuel litige, ce dernier devra contrôler de manière systématique la liste des certificats révoqués qu'aura émis le PSCE, vérifier la signature (ce qui sous entend l'intégrité du message) et le certificat électroniques (sa date d'expiration et le chemin de confiance). Enfin, il devra archiver l'ensemble de ces éléments, pour pouvoir apporter la preuve de ces diligences dans le cadre d'un éventuel contentieux ; mais il peut également avoir recours à une autorité de validation de gestion de preuve (AGP).

Actuellement, les certificats électroniques ne contiennent pas de champs prévus pour inscrire les limites d'utilisation et de valeur — et cela n'est pas sans incidence sur les risques qui pèsent sur les PSCE. En ce qui concerne les signatures qui se fondent sur des certificats non qualifiés ainsi que pour toutes les autres obligations, c'est le droit commun qui s'applique : les articles 1382 et suivants du Code civil pour la responsabilité délictuelle et le droit des obligations contractuelles pour les rapports entre le PSCE et son client [58].

Le dernier alinéa de l'article 33 dispose également que le PSCE devra justifier d'une garantie financière ou d'une assurance « garantissant les conséquences pécuniaires de sa responsabilité civile ». Cette exigence, peut être d'une application pratique délicate dès lors que le risque financier est relatif au montant et à la nature spécifiques à chaque préjudice ainsi qu'aux limites contenues dans le certificat. C'est donc une appréciation *in concreto* qui devra être effectuée [59].

En tout état de cause, actuellement les premiers certificats électroniques qualifiés apparaissent (Banque de France, certains actes authentiques).

Tout ce dispositif ne doit pas masquer le fait que les signatures électroniques sécurisées ne représentent qu'une part minime au sein de toutes les applications de signatures électroniques. Si les premières doivent permettre aux signataires de disposer d'une signature *a priori* fiable devant les tribu-

58. Pour de plus amples renseignements sur la responsabilité de plein droit, v. Ph. le Tourneau, *op. cit.*

59. J.-L. Santoni, « Comment assurer l'activité de certification de signature électronique », *Expertises des systèmes d'information* 2005. 291. 137 s.

naux, les secondes pourront également être utilisées dans le cadre du commerce électronique, quitte pour les signataires à démontrer leur fiabilité devant le juge, ce qui nécessitera l'intervention active du PSCE en possession de tous éléments nécessaires à la démonstration de la fiabilité du procédé de signature utilisé.

Néanmoins, pour se développer, la confiance s'appuiera à la fois sur la sécurité de l'infrastructure au travers des technologies employées (à base d'outils liés à la cryptographie) et sur la sécurité juridique qui s'exprime par leur cadre juridique et des règles spécifiques de responsabilité. Sur le plan géographique, il faudra que les technologies soient interopérables et que le cadre juridique soit sinon unifié, à tout le moins harmonisé comme c'est le cas dans l'Union européenne. La signature électronique est un outil de la confiance qui s'est construit avec les actions conjuguées du droit, de la technique et de l'organisation.

Nice, le 31 août 2005