Rubrique : chroniques francophones / volume 2 / France
Mots clés : preuve, signatures, électroniques, contrats, actes, commerce
Citation : Valérie SÉDALLIAN, "Preuve et signature électronique", Juriscom.net, 9 mai 2000
Première publication : Juriscom.net, article présenté lors du séminaire franco-allemand organisé par l'Association Française des Avocats Conseils d'Entreprises et le Deutscher Anwalt Verein à Nice, le 14 et 15 avril 2000.

Preuve et signature électronique

Par Maître Valérie Sédallian
Avocate à la Cour de Paris
www.internet-juridique.net

email : sedallian@argia.fr

Introduction

1. Partant du constat du développement du commerce électronique et de la nécessité d'assurer un cadre juridique sûr aux transactions électroniques, le gouvernement a présenté un projet de loi visant à adapter le droit de la preuve aux technologies de l'information et relatif à la signature électronique. Ce projet de loi a été présenté comme un des volets essentiels de l'action du gouvernement pour adapter la législation aux nouveaux enjeux de la société de l'information. Le texte adopté par la commission des lois du sénat1[1], après avoir été voté à l'unanimité par le Sénat le 8 février 2000, a été adopté dans des termes identiques par l'Assemblée Nationale le 29 février 20002[2]. La loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique3[3] vient ainsi d'être adoptée.

2. Comme cela a été souligné à de nombreuses reprises, la loi française s'inscrit dans un contexte international. Depuis plusieurs années, les organisations internationales se préoccupent de la reconnaissance du document et de la signature électronique. L'impulsion est venue de la *Commission des Nations Unies pour le droit commercial international* (CNUDCI). La loi-type sur le commerce électronique a été adoptée le 16 décembre 1996 par l'Assemblée Générale, alors qu'un projet de règles uniformes sur les signatures électroniques est en cours d'élaboration4[4]. Au niveau communautaire, la directive fixant un cadre juridique pour les signatures électroniques a été adoptée le 13 décembre 19995[5]. Le projet de directive relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, qui traite entre autres questions des contrats par voie électronique (article 9), vient de faire l'objet

1[1] Rapport de M. Charles Jolibois, n° 203.

2[2] Rapport de M. Christian Paul, n° 2197.

3[3] JO du 14 mars 2000.

4[4] « Droit de la preuve et signature électronique », Aperçu rapide, *JCP G* 15 mars 2000, p. 451.

5[5] Directive 1999/93/CE, JOCE du 19 janvier 2000, <http://europa.eu.int/comm/internal_market/fr/media/index.htm>.

d'un accord politique du Conseil de l'Union en date du 7 décembre 19996[6]. En France, le dépôt du projet de loi a été précédé de nombreux travaux7[7], notamment ceux d'un groupe de travail constitué par le GIP « *Droit et Justice* »8[8], à la demande de la Chancellerie, qui a élaboré une première version du texte qui a servi de base à l'avant-projet de loi.

3. La preuve est un élément essentiel de tout système juridique. Le droit français de la preuve s'organise autour de la référence à l'écrit et est marqué par le principe de prééminence de l'écrit. Même si le contrat est valablement formé sans écrit du seul fait de l'échange des consentements des parties, la nécessité pour les parties de se ménager la preuve de leur contrat impose en réalité le recours à un écrit.

4. L'écrit au sens traditionnel, c'est le titre original revêtu d'une signature manuscrite et matérialisé dans un document papier. La jurisprudence a toutefois permis certaines évolutions. La validité des conventions de preuve a ainsi été reconnue dans un arrêt du 8 novembre 1989 de la Cour de cassation9[9] (affaire *Crédicas*), à propos des cartes de paiement et de crédit, et plus récemment, un arrêt remarqué de la Chambre commerciale du 2 décembre 199710[10] a clairement énoncé les conditions nécessaires à la valeur probatoire d'un document produit par télétraitement à propos d'un acte d'acceptation de cession d'une créance professionnelle : « *l'écrit… peut être établi et conservé sur tout support, y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées*. »

5. Cependant, cette jurisprudence n'était pas applicable dans le cas de transactions conclues en « milieu ouvert », c'est-à-dire sans qu'un accord préalable ait été conclu entre les parties. En outre, l'utilisation des échanges électroniques n'est plus limitée au seul droit des affaires. De l'avis unanime de la doctrine, une réforme s'imposait, le droit en vigueur n'étant pas adapté aux échanges électroniques.

6. Le texte qui a été adopté modifie les règles du Code civil relatives à la preuve, en consacrant la valeur probante de l'écrit sous forme électronique, d'une part, et en introduisant la signature électronique dans notre droit, d'autre part. La loi est saluée comme constituant une avancée fondamentale du droit de la preuve. Pourtant, l'apport de la loi reste limité au domaine de la preuve, et de nombreuses questions techniques devront être résolues avant que l'écrit électronique ne puisse se substituer effectivement aux échanges de documents sur « papier ».

I. La preuve et la signature électronique

A. Les apports de la loi à la reconnaissance juridique de la preuve électronique

7. La loi comporte deux volets particulièrement novateurs : la redéfinition de la preuve littérale et la consécration de la force probante de l'écrit électronique.

6[6] 14263/1/99 REV 1, disponible sur le site de la Direction générale du Marché intérieur : <http://europa.eu.int/comm/internal_market/fr/media/index.htm>.

7[7] Conseil d'Etat, *Internet et les réseaux numériques*, La Documentation française 1998, p. 79-96 ; Conseil National du Crédit et du Titre, *Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres*, mai 1997.

8[8]Voir : « L'introduction de la preuve électronique dans le Code civil », Etude par un groupe d'universitaires, *JCP G* 1999, I, 182.

9[9] 1ère Civ. 8 novembre 1989, Bull. Civ. I, n° 342 ; *JCP* G 1990, II, 21576, note G. Virassamy.

10[10] JCP E 1998, p. 178, note T. Bonneau.

1. La redéfinition de la preuve littérale

8. Selon le nouvel article 1316 du Code civil : « *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 ».*

9. La définition de la preuve par écrit est donc extensive, ce qui valide toutes formes d'écrits, y compris mais non exclusivement ceux sous forme électroniques. Traditionnellement, l'écrit avait fini par se confondre avec son support papier. Pourtant, le dictionnaire définit l'écriture comme « *une représentation de la parole et de la pensée par des signes* », sans qu'il soit fait référence à un quelconque support papier. La loi met donc fin à cette confusion : la preuve littérale est redéfinie afin de la rendre indépendante de son support. La preuve littérale ne s'identifie plus au papier, ne dépend ni de son support matériel, ni de ses modalités de transmission. La définition respecte ainsi le principe de neutralité technologique11[11].

10. La suite de signes constituant l'écrit doit être ordonnée de manière à être intelligible : l'écrit doit pouvoir être produit de façon lisible et compréhensible par l'homme. Un texte peut être crypté, mais il doit pouvoir être déchiffré pour posséder une vocation probatoire12[12].

2. La consécration de la force probante de l'écrit électronique

11. Selon le nouvel article 1316-1 : « *L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».* L'article 1316-3 précise : « *L'écrit sur support électronique a la même force probante que l'écrit sur support papier »*.

12. Ainsi, le législateur n'a pas voulu instituer de hiérarchie entre support électronique et support papier. L'avant-projet de loi prévoyait que : « *la preuve contraire peut être rapportée contre un écrit électronique sur le fondement de présomptions graves, précises et concordantes*. » Il s'agissait d'un point controversé, certains considérant que donner aux preuves informatiques la même force probante qu'aux écrits traditionnels sur support papier aurait été prématuré13[13], d'autres considérant au contraire que cela remettait en cause l'objectif même qui était poursuivi14[14]. L'admission d'un écrit sous forme électronique en tant que preuve au même titre que l'écrit papier est consacrée à la double condition que puisse être identifié celui dont il émane et que les conditions dans lesquelles il est établi et conservé en garantissent l'intégrité.

13. Pour les actes unilatéraux, l'article 1326 du Code civil prévoyait la mention manuscrite de la somme en toutes lettres et en chiffres. Désormais, les mots « de sa main » sont remplacés par les mots : « par lui-même ».

3. Règlement des conflits de preuve

11[11] Eric Caprioli, « Le juge et la preuve électronique », *Juriscom.net*, 10 janvier 2000, <http://www.juriscom.net>.

12[12] « L'introduction de la preuve dans le Code civil », étude précitée, n° 6.

13[13] « L'introduction de la preuve dans le Code civil », étude précitée, n° 11.

14[14] P. Leclercq, « Propositions diverses d'évolutions législatives sur les signatures électroniques », *Droit de l'informatique et des télécommunications*, 1998/3, p. 19 ; Eric Caprioli, « Le juge et la preuve électronique », préc.

14. Il est inséré dans le Code civil un article 1316-2 précisant qu'il appartiendra souverainement au juge de déterminer au cas par cas, en tenant compte des circonstances de l'espèce, quelle est la preuve littérale la plus vraisemblable.

15. Un arrêt récent de la 1ère Chambre de la Cour de cassation, en date du 15 février 200015[15], rappelle que conformément aux articles 287, 288 et 289 du Nouveau code de procédure civile, lorsque la partie à laquelle on oppose un acte sous seing privé en dénie l'écriture et la signature, il appartient au juge de vérifier l'acte contesté et de procéder à la vérification d'écriture au vu des éléments dont il dispose, après avoir, s'il y a lieu, enjoint aux parties de produire tous documents à comparer à cet acte.

4. Consécration de la validité des conventions sur la preuve

16. Le législateur a consacré la jurisprudence dite « *Credicas* »16[16] qui avait reconnu la possibilité de passer des conventions sur la preuve. La loi n'a pas fixé les conditions de validité minimales de ces conventions.

17. Les principes relatifs aux clauses abusives sont toutefois parfaitement applicables : entre professionnel et non professionnel, la convention sur la preuve ne doit pas constituer une clause dite abusive17[17]. Or, les moyens de preuve sont détenus par l'exploitant du système. Une recommandation de la Commission des clauses abusives demande par exemple que soient éliminées des contrats « porteurs » proposés par les émetteurs de cartes, les clauses ayant pour objet ou pour effet « *de conférer aux enregistrements magnétiques détenus par les établissements financiers ou bancaires une valeur probante en dispensant ces derniers de l'obligation de prouver que l'opération contestée a été correctement enregistrée et que le système fonctionnait normalement* »18[18].

B. La signature électronique

1. La reconnaissance juridique de la signature électronique

> La signature d'un point de vue fonctionnel

18. La signature n'était pas définie en droit français, même si le Code civil mentionne à plusieurs reprises l'obligation d'une signature : article 1322 sur les actes sous seing privé, article 1325 sur le contrat synallagmatique et la formalité du double original, article 1326 sur la reconnaissance de dette.

19. La signature remplit deux fonctions juridiques de base :

- identification de l'auteur ;

- manifestation de sa volonté, approbation du contenu de l'acte.

20. L'article 1316-4 introduit dans le Code civil une définition de la signature : « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le*

15[15] N° C 98-12.032, Lecornec c/ Udeco diffusion.

16[16] Voir supra note n° 9.

17[17] Article L 132-1 du Code de la consommation ; directive 93/13 du 5 avril 1993.

18[18] Recommandation n° 94-02 relative aux contrats porteurs des cartes de paiement, BOCCRF 30 mai 1995, p. 182

consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte ». Encore une fois, cette définition est neutre : elle vaut pour toutes formes de signature qu'elle soit manuscrite, électronique ou autre. Il s'agit d'une définition dite fonctionnelle19[19] : le nouvel article donne une définition générale des fonctions de la signature.

> *La signature électronique*

21. Le deuxième alinéa de l'article 1322-2 traite du cas où la signature est électronique : « *Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »*

22. La validité de la signature numérique par saisie d'un code associé à une carte de paiement a été reconnue dans le cadre de la jurisprudence sur les conventions de preuve20[20]. Le texte va plus loin en consacrant la validité de la signature électronique en l'absence de toute convention préalable. La signature électronique sera présumée fiable dès lors qu'elle remplira certaines conditions qui devront être précisées par un décret en Conseil d'Etat. Ces décrets viseront à mettre en œuvre les dispositions de la directive sur la signature électronique avancée, et notamment celles relatives aux prestataires de services de certification.

23. Cette directive vise à faciliter l'utilisation des signatures électroniques, à contribuer à leur reconnaissance juridique et à instituer un cadre juridique pour les services de certification. Elle définit un ensemble de critères qui constituent la base de la reconnaissance juridique de la signature électronique. Elle institue notamment le principe de non-discrimination entre signature électronique et manuscrite (article 5).

24. La signature n'est pas définie de manière abstraite, mais se rattache à des données (article 2). La directive distingue « la signature électronique » de « la signature électronique avancée ». La signature électronique est définie comme « *une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification* ».

25. Ici, la signature électronique est conçue comme un moyen technique de sécurisation, elle n'est pas définie par rapport à ses effets juridiques, mais par rapport à ses effets techniques. Elle recouvre également des processus techniques d'authentification entre ordinateurs, qui n'ont pas nécessairement de signification juridique. Cette définition technique de la signature n'a pas été reprise dans la loi française.

26. La signature électronique avancée respecte les exigences suivantes :

- « *être liée uniquement au signataire ;*
- *permettre d'identifier le signataire ;*
- *être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; et*
- *être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.* »

19[19] Eric Caprioli, « Le juge et la preuve électronique », préc.

20[20] Voir supra note n° 9.

27. La signature électronique avancée, telle qu'elle est envisagée par le texte de la directive, est la signature numérique basée sur la cryptologie à clé asymétrique. Le contexte technologique de la signature électronique est en effet complexe.

28. Il existe deux grands types de cryptographie :

- la cryptographie symétrique : la même clé est utilisée pour chiffrer et déchiffrer l'information. Le problème de cette méthode est qu'il faut trouver le moyen de transmettre de manière sécurisée la clé à son correspondant ;

- la cryptographie asymétrique : ce n'est pas la même clé qui crypte et qui décrypte les messages. L'utilisateur possède une clé privée et une clé publique. Il distribue sa clé publique et garde secrète sa clé privée. La clé privée ne peut pas être recomposée à partir de la clé publique. Les méthodes de cryptage à clés asymétriques reposent sur des calculs mathématiques sophistiqués utilisant des nombres premiers générés par des algorithmes. Il est facile de multiplier deux nombres premiers par exemple 127 et 997 et de trouver 126 619. Mais il est plus difficile de factoriser c'est-à-dire de retrouver 127 et 997 à partir de 126 619.

29. Comment ce système permet-il de gérer une signature ? L'utilisateur A signe avec sa clé privée son message. Tout le monde peut vérifier qu'il est bien l'auteur du message en comparant la signature du message avec la clé publique correspondant à l'expéditeur ainsi identifié.

30. Pour vérifier l'intégrité du message transmis, le caractère exact et complet des données envoyées, on utilise une fonction mathématique qui associe une valeur calculée au message. Lorsque le destinataire reçoit le message, il calcule sa propre valeur et la compare avec celle qui lui a été envoyée : si les deux valeurs sont identiques, on est assuré que les documents n'ont pas été modifiés.

31. La combinaison de procédés d'authentification de l'expéditeur et de vérification de l'intégrité de son message permet la création de véritables signatures électroniques. Elle repose sur la mise en œuvre d'outils informatiques.

32. Les procédés de cryptographie à clé publique fournissent ainsi une solution au problème d'identification des interlocuteurs échangeant des messages en milieu ouvert. Ce système peut nécessiter l'intervention d'un tiers : le tiers certificateur, dont le rôle va consister à administrer et publier les clés publiques21[21].

2. Les prestataires de services de certification

33. Le tiers certificateur permet de s'assurer qu'une clé publique est bien celle du correspondant, et donc de vérifier son identité et ses pouvoirs. En l'absence d'un réseau de certification, la question des échanges entre personnes qui ne sont jamais rentrées en relation auparavant reste entière : comment ces personnes vont-elles échanger de manière sécurisée leurs clés publiques, qui garantira que la clé donnée est bien celle de la personne annoncée et non pas celle d'un imposteur ? Sans certitude sur l'identité du cocontractant, la validité de la signature et donc de la transaction peut être contestée. Il existe actuellement des serveurs de clés publiques22[22], mais qui ne fournissent pas toujours de garanties quant à la vérification de l'identité des déposants.

34. Pour que le recours au système de cryptage à clé publique offre une sécurité juridique, des réseaux de certification doivent être mis en place. Le tiers certificateur est un organisme, public ou privé, qui émet des certificats électroniques. Le certificat est un registre informatique revêtu d'une

---

21[21] Eric A. Caprioli, « Sécurité et confiance dans le commerce électronique, signature numérique et autorité de certification », *JCP G* 1998, I, 123.

22[22] Voir par exemple le site de la société Verisign : <http://www.verisign.com>.

signature électronique qui identifie l'émetteur du certificat, identifie le souscripteur et donne sa clé publique. Il s'agit d'une sorte de carte d'identité électronique qui serait émise par un tiers indépendant et neutre. La signature électronique correspondant à un certificat est considérée appartenir à la personne mentionnée dans le certificat.

35. Un certificat peut permettre de vérifier l'identité d'une personne, mais également ses pouvoirs et sa capacité, ses qualifications professionnelles (par exemple il sera possible de vérifier si la personne est bien médecin, avocat...), le pouvoir d'engager une société. La directive sur les signatures électroniques vise à instaurer une reconnaissance communautaire des services de certification des signatures électroniques.

36. D'après une recommandation n° 509 de l'*UIT-T*, une autorité de certification est « *une autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat*. » Il a pour fonction de formaliser le lien qui existe entre une personne physique ou morale et une paire de clés asymétrique.

37. Dans la directive, les tiers certificateurs sont appelés « prestataires de services de certification » (ci-après PSC). Le PSC est défini comme : « *toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques*. » La directive définit le certificat comme *« une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne.* Le certificat doit répondre à des exigences fixées par l'annexe I de la directive.

38. Le champ d'application de la directive est plus large que celui des seules autorités de certification qui délivrent des certificats liés à la signature électronique. Les prestataires de la directive pourront fournir également des services d'horodatage, d'archivage, des services de publications et de consultation etc… Cette activité ne fait l'objet d'aucune réglementation spécifique en droit français, hormis en ce qui concerne la réglementation de la cryptologie. La directive, intégrée dans notre législation, donnera un cadre juridique à ces services.

> La fourniture de services de certification

39. La fourniture de services de certification ne pourra être soumise à aucune autorisation préalable (article 3 de la directive). Les états peuvent prévoir un processus de reconnaissance professionnelle ou accréditation pour l'exercice de la mission de PSC23[23]. Cependant, la procédure d'accréditation repose sur le volontariat et n'aurait pas de caractère obligatoire. Le décret régira le système d'accréditation volontaire des autorités de certification, conformément à la directive.

40. Par ailleurs, l'annexe II de la directive fixe un certain nombre d'exigences auxquelles doivent satisfaire les PSC, parmi lesquelles :

- assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat ;

- vérifier, par des moyens appropriés et conformes au droit national, l'identité de la personne à laquelle le certificat est délivré ;

- utiliser des systèmes fiables ;

- archiver les informations relatives aux certificats pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice ;

23[23] Thierry Piette-Coudol, « Vers la reconnaissance juridique de la signature électronique », *Cahiers Lamy Droit de l'Informatique*, n° 104, juin 1998.

- disposer de ressources financières suffisantes.

> La responsabilité des PSC

41. Il doit exister des garanties juridiques pour le cas où le PSC manquerait à ses obligations. La question de la responsabilité du PSC est particulièrement sensible lorsque le certificat est erroné. La directive prévoit la responsabilité des PSC sur l'exactitude des informations certifiées par eux et sur l'imputabilité de la signature à la date où le certificat a été délivré (article 6). C'est au prestataire de service de prouver qu'il n'a commis aucune négligence. Or, une preuve négative est très difficile à rapporter… D'une manière générale, le PSC a l'obligation d'assurer la sécurité du système mis en place (voir les Exigences concernant les PSC, Annexe II).

> Libre circulation des produits

42. Les services établis dans un Etat et les éventuelles accréditations délivrées par un Etat devront être reconnus dans les autres Etats. Les produits de signature électronique doivent pouvoir circuler librement sur le marché intérieur.

> Aspects internationaux

43. Dans la perspective de la mise en place d'un système de reconnaissance mutuelle des signatures et certificats avec les pays tiers, la directive prévoit les conditions pour que les certificats délivrés par un PSC d'un pays tiers soient juridiquement reconnus comme équivalents aux certificats délivrés par un PSC établi dans la Communauté européenne. En particulier, un PSC établit dans la Communauté pourra garantir les certificats d'un PSC d'un pays tiers.

44. En conclusion, cette directive sur les signatures électroniques est très technique.

II. Les limites de la réforme

45. Le changement apporté par la loi est fondamental dans son principe, mais limité aux aspects probatoires, alors que de nombreuses questions concrètes devront être résolues avant la mise en œuvre effective de la réforme.

A. La loi ne concerne que les aspects probatoires

46. Les travaux législatifs et les premiers commentaires soulignent que la loi ne concerne que les aspects probatoires et la signature des actes juridiques, mais non les questions touchant à la validité des actes24[24]. Les dispositions de la loi sont insérées dans le Code civil à l'intérieur des textes relatifs à la preuve. Lorsqu'un écrit est exigé sur support papier *ad validitatem*, la loi n'apporte aucune modification au régime actuel. Il en va ainsi par exemple des dispositions relatives au démarchage à domicile25[25], des contrats de crédit à la consommation ou de crédit immobilier26[26].

47. Il en va de même évidemment pour les actes solennels pour lesquels l'intervention d'un notaire est obligatoire, tels les actes de mariage ou les donations. Certes, l'article 1317 du Code civil a été modifié afin de préciser que l'acte authentiques peut être dressé sur support

---

24[24] Jérôme Huet, « Vers une consécration de la preuve et de la signature électronique », *Dalloz* 6 janvier 2000 ; Luc Grynbaum, « La preuve littérale et la signature à l'heure de la communication électronique », *Communication, Commerce Electronique*, novembre 1999, ch. p. 9.

25[25] Articles L 121-23 et L 121-24 du Code de la consommation.

26[26] Articles L 31-8 et L 312-8 du Code de la consommation.

électronique. Il est toutefois précisé « *s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat*. » Les actes authentiques ont été inclus dans le champ d'application de la loi sur proposition de la commission des lois du Sénat27[27], tout en renvoyant la question de sa mise en œuvre pratique à des décrets. Il s'agit de ne pas exclure les actes authentiques des nouvelles technologies de l'information. Cependant, les débats devant le Sénat soulignent que les techniques nécessaires à une dématérialisation des actes authentiques ne peuvent pas être mises en oeuvre, l'acte authentique devant par exemple être conservé pour une durée illimitée, alors que les techniques actuelles ne permettent de garantir la conservation des informations que pour une durée limitée, en raison de leur obsolescence rapide. La Ministre de la Justice a ainsi souligné que : « *il est clair que le décret ne pourra être publié rapidement*.28[28] »

48. Cette exclusion est conforme à la directive qui précise bien qu'elle ne couvre pas les aspects liés à la conclusion et la validité des contrats ou d'autres obligations légales lorsque des exigences d'ordre formel sont prescrites par la législation nationale ou communautaire (article 1 al.2).

B. La mise en œuvre concrète des principes prévus est nécessaire

1. Les conditions de la force probante de l'écrit et de la signature électronique sont liées à la fiabilité des systèmes et à l'intégrité des données

49. La sécurité des systèmes informatique constitue un enjeu essentiel et un débat permanent. Or, toutes les questions techniques essentielles à la mise en œuvre des conditions posées par la loi sont loin d'être réglées.

50. En premier lieu, le marché des services de certification n'en est encore qu'à ses débuts et reste très orienté vers les entreprises. Les infrastructures à clés publiques sont complexes et onéreuses, bien qu'elles soient apparues il y a déjà une dizaine d'années, et restent peu utilisées29[29]. En second lieu, les aléas techniques sont nombreux en matière informatique.

51. Par nature, la sécurité est le point faible des réseaux ouverts. Pour certains auteurs, « *les preuves électroniques sont, aujourd'hui encore, trop unilatéralement établies et archivées, sans garantie de sécurité parfaite, ni même de détection, contre les risques de fraudes, émanant d'employés indélicats, voire de tiers intrus…* 30[30]». D'autres soulignent encore que la notion de fiabilité du support informatique est imparfaite et opère une discrimination entre utilisateurs institutionnels, entreprises et consommateurs31[31]. La généralisation de l'utilisation de documents électroniques nécessite au préalable la généralisation des moyens techniques de sécurisation.

2. La conservation

27[27] Voir supra note n°1.

28[28] Compte rendu analytique de la séance du 8 février 2000, sur le site du Sénat : <http://www.senat.fr> .

29[29] Marie Varandat, « Consolidation des infrastructures à clés publiques avant leur prochain décollage », *01 Informatique*, 10 mars 2000 p. 22.

30[30] Pierre Leclercq, art. préc. p. 20.

31[31] Cyrille Charbonneau, Frédéric-Jérôme Pansier, « Le droit de la « preuve » est un totem moderne (le commerce électronique) », *Gaz. Pal*. 31 mars 2000, p. 2.

52. La force probante de l'écrit électronique est notamment subordonné à la condition qu'il soit conservé dans des conditions de nature à en garantir l'intégrité. La question de la conservation est indissociable de la question de la preuve et correspond à un besoin pratique réel. Comment se servir de la preuve électronique si la conservation afférente aux documents électronique n'est pas résolue ?

53. La conservation des moyens de preuve sur des durées couvrant la prescription des actes les plus courants, soit au moins jusqu'à à dix ans en matière commerciale est donc fondamentale. Les données sous forme électronique doivent être archivées dans des conditions offrant des garanties de sécurité contre toute altération, modification ou destruction. L'archivage correspond à l'idée de pérennité de l'information avec la possibilité de la restituer intacte. Or, l'informatique ne poursuit pas ces finalités. L'enjeu consiste donc à fournir des garanties de sécurité tout en remplissant les fonctions juridiques traditionnelles attachées au papier, mais dans un univers informatique32[32].

54. Techniquement, il existe de nombreuses difficultés. Par exemple, compte tenu de l'évolution rapide des techniques, il est difficile de garantir que l'on disposera au moment voulu des interfaces logicielles et matérielles requises pour accéder à la lecture du document électronique établi dix ans plus tôt. De même, compte tenu de la rapidité des progrès technologiques, il existe un risque non négligeable que la technologie utilisée pour les clés de signature ne devienne obsolète, par exemple que la clé privée puisse être recalculée à partir de la clé publique33[33].

55. Les prestataires de services de certification doivent enregistrer et archiver les informations pertinentes concernant un certificat pendant le « délai utile », c'est-à-dire le délai nécessaire pour pouvoir fournir une preuve de la certification en justice. (point I de l'annexe II de la directive). Cet archivage ne couvre pas les écrits eux-mêmes revêtus d'une signature électronique : cette conservation ne concerne que le certificat correspondant à la signature liée au document électronique.

56. L'*AFNOR* a publié des recommandations relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes34[34]. Cette norme fixe des directives techniques, des consignes d'exploitation, de sécurité, de traçabilité des documents numérisés. Elle décrit les types de support à utiliser, à savoir les disques optiques non réinscriptibles dits « WORMS »35[35]. Cette norme suppose une certification ISO du système d'archivage. Concernant le problème de la durabilité en longue période des enregistrements, la norme préconise la recopie périodique (mais il faut pouvoir recopier à la fois les logiciels et les données).

57. Elle montre en tout état de cause que la mise en œuvre de moyens techniques d'archivage de documents électroniques offrant des garanties de sécurité et d'intégrité est un métier éminemment technique, relevant de professionnels de l'informatique.

58. La conservation des moyens de preuve risque pour une large part d'être unilatérale, car les fournisseurs de produits et services seront souvent les seuls à pouvoir archiver sur de longues durées. Le cocontractant risque de ne pas disposer des équipements permettant de le faire de façon systématique, voire satisfaisante36[36]. C'est la raison pour laquelle certains pensent que

---

32[32] Eric Caprioli, « Variations sur le thème de l'archivage dans le commerce électronique », *Petites Affiches* du 18 août 1999, p. 4 et du 19 août 1999 p. 7.

33[33] Eric Caprioli, « Le juge et la preuve électronique », préc.

34[34] Norme ISO Z 42-013, juin 1998.

35[35] Write once read many.

36[36] Huet, art. préc.

les prestataires de services de certification seront amenés également à proposer des services d'archivage37[37].

3. La date

59. Sauf texte spécial, la date d'un acte n'est pas une condition de validité de cet acte. Néanmoins, l'indication de la date d'un acte est une énonciation essentielle38[38]. Le moment de conclusion du contrat marque le point de départ des effets de l'acte. Le temps influe également sur le droit lorsqu'il s'agit de déterminer un délai39[39]. Par exemple, il est courant qu'un contrat à durée déterminée renouvelable par tacite reconduction puisse être résilié dans un délai de quelques mois précédant la date anniversaire du contrat.

60. Autre exemple, en matière de marchés publics, le délai de remise du dossier de candidature à un appel d'offres doit impérativement être respecté. Il n'existe pas de dispositions particulières dans le Code civil relativement à la force probante de la date à l'égard des parties contractantes. Entre les parties, les actes sous seing privé font foi de leur date, comme de leur contenu, jusqu'à preuve contraire. Or, en matière informatique, la date indiquée dans un message ne présente aucune garantie. Il est aisé pour l'utilisateur de modifier la date de l'horloge interne de son ordinateur. Même si l'horloge de son ordinateur était correctement réglée au départ, elle doit être régulièrement remise à l'heure, car l'horloge « dérive ». Le problème s'accentue en cas d'équipements fonctionnant en réseau, comme c'est le cas sur Internet, car les différents ordinateurs intervenant lors d'une communication donnée peuvent avoir des dates différentes.

61. La sécurité des rapports contractuels peut en être affectée. Surtout, chaque fois qu'une échéance impérative est calculée à partir d'une date, il est nécessaire de pouvoir se référer à une date « certifiée ». Il existe des protocoles qui permettent la synchronisation permanente des serveurs à des horloges de référence40[40]. Il est donc nécessaire d'avoir recours à des services d'horodatage des messages qui pourront garantir la date des actes juridiques sous forme électronique41[41]. Là encore, ces services d'horodatage pourront être proposés par les prestataires de certification.

C. Le texte permet-il de remédier aux difficultés liées aux transactions sur Internet ?

62. Les débats parlementaires soulignent que la loi va permettre d'offrir des garanties aux consommateurs sur Internet et dynamiseront le développement du « cyber-commerce ». En effet, les internautes français seraient particulièrement réticents à effectuer leurs achats sur Internet. En pratique, la loi risque d'avoir peu d'influence sur cette question.

63. L'achat en ligne de biens ou de prestations fait intervenir deux actes juridiques distincts : le paiement et le contrat de vente ou de services. S'agissant du contrat lui-même, sauf pour certains contrats spécifiques nécessitant un formalisme particulier, aucune forme particulière n'est requise pour la validité du contrat : c'est le principe bien connu du consensualisme qui couvre les contrats

---

37[37] Eric Caprioli, « Variations sur le thème de l'archivage dans le commerce électronique », art ; préc.

38[38] Pierre Strasser, « Force probante de la date d'un acte sous seing privé », *Juris. Cl. Civil Fasc*. 142.

39[39] Emmanuel Putman, « Le temps et le droit », *Droit & Patrimoine*, janvier 2000, p.43.

40[40] Voir Services de temps, disponible sur le site du CRU (Comité Réseau des Universités) à l'adresse : <http://www.cru.fr/NTP>.

41[41] Eric Caprioli, « Le juge et la preuve électronique », préc.

courants. La conclusion de contrats par voie électronique est tout à fait possible, pourvu que soit adaptée l'expression du consentement.

64. Au niveau de la preuve du contrat, il faudrait respecter les exigences de la loi qui prévoit que l'écrit sous forme électronique doit permettre d'identifier la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. Sur le deuxième point, nous avons vu qu'elle suppose que les fournisseurs mettent en place les procédures techniques adéquates pour conserver et sécuriser les données reflétant les opérations de leur commerce électronique.

65. Sur le premier point, seule l'utilisation d'une signature électronique permet aujourd'hui d'assurer cette fonction d'identification en l'absence de relation contractuelle préalable. Or, la généralisation des signatures électroniques sur Internet suppose la mise en œuvre effective des services de certification. Cette certification sera génératrice de coût et d'un certain formalisme. Comme le soulignent certains : « *il est douteux que les menues opérations de la vie courante s'accommodent de ces complications. On peut donc sans être mage ou devin, prévoir que le commerce électronique comportera des sécurités à étage, et que des millions d'opérations continueront de se faire à découvert, c'est-à-dire avec risque, comme il en va des chèques et des cartes de crédit*. »42[42]

66. En réalité, c'est le paiement sur Internet qui focalise les craintes des consommateurs. Le mode de paiement le plus couramment utilisé sur Internet consiste à indiquer le numéro apparent de sa carte bancaire, en général crypté avec le protocole SSL intégré au navigateur. Beaucoup craignent que leur numéro de carte ne soit intercepté et utilisé à leur insu. Pourtant, le consommateur dispose d'un recours auprès de sa banque en cas d'utilisation frauduleuse de sa carte.

67. L'écho donné par les médias à l'affaire *Humpich*43[43], concernant cet informaticien qui aurait trouvé une faille dans le système de sécurité des cartes à puces utilisées en France pour les cartes de paiement, bien qu'elle concerne un problème différent puisque lié au code confidentiel qui n'est pas communiqué dans le cadre d'un paiement en ligne, n'est pas fait pour rassurer le grand public.

68. La loi, qui est relative au problème de la preuve, ne règle pas cette question de la crainte des piratages et de la nécessaire sécurisation des systèmes de paiement sur Internet. Au demeurant, le titulaire du compte est déjà lié par une convention de preuve avec sa banque. Ainsi, les conditions générales de fonctionnement des cartes bleues indiquent : « *le titulaire du compte autorise la banque à débiter son compte au vu des enregistrements ou des relevés transmis par le commerçant, même en l'absence de factures signées par le titulaire de la carte ou assorties d'un contrôle du code confidentiel, pour le règlement des achats de biens ou de prestations de services* »44[44].

69. Cette pratique contractuelle est simplement confortée par la loi qui entérine la validité des conventions de preuve. Sur la preuve du paiement, la loi n'apporte aucune modification majeure, la convention de preuve liant la banque au consommateur détenteur de la carte de crédit et non celui-ci au commerçant45[45].

42[42] « L'introduction de la preuve dans le Code civil », étude précitée n° 9.

43[43] Voir sur cette affaire le site : <http://www.parodie.com>.

44[44] article 7.5, édition janvier 1999.

45[45] Théo Hassler, « Preuve de l'existence d'un contrat et Internet : brèves observations à propos d'une proposition de loi », *Juriscom.net*, 16 juillet 1999, <http://www.juriscom.net> ; *Petites affiches* 21 septembre 1999, p. 4.

D. La cohérence avec la réglementation de la cryptologie

70. Il est difficile d'aborder la réglementation de la signature électronique et des services de certification sans évoquer la réglementation de la cryptographie : la cryptographie apporte la sécurité technique nécessaire à la signature, la fourniture de services de certification est liée aux techniques de cryptographie asymétrique.

71. La loi française n° 96-659 du 26 juillet 199646[46] repose sur la dichotomie entre les fonctions d'authentification et d'intégrité, soumise à un régime plus libéral, et les fonctions de confidentialité, sur lesquelles l'Etat entend garder un contrôle étroit. Elle prévoit pour l'utilisation de la cryptographie forte à des fins de confidentialité le recours au système des tiers de confiance47[47].

72. La France dispose d'une réglementation complexe et de la plus stricte des pays développés. Dans une conférence de presse du 19 janvier 1999 sur la Société de l'Information, le Premier ministre a annoncé la refonte de la législation adoptée en 1996. Il est notamment envisagé de supprimer le caractère obligatoire du recours aux tiers de confiance. D'ores et déjà, en attendant la modification législative annoncée, deux décrets et un arrêtés publiés le 17 mars 199948[48] ont relevé le seuil de la cryptologie dont l'utilisation est libre de 40 bits à 128 bits.

73. Un prestataire de services de certification sera aux termes de la loi française un fournisseur de prestation de cryptologie. Si la simple utilisation d'une signature électronique est libre, il n'en va pas de même pour la fourniture qui est soumise à la formalité de la déclaration préalable. Les fonctionnalités utilisées pour l'authentification et le contrôle de l'intégrité ne doivent pas permettre de chiffrer d'autres informations que les données nécessaires au contrôle d'accès, ni aucune autre information que celle nécessaire à l'authentification ou au contrôle d'intégrité des données elles-mêmes. Sinon, le produit relève de la formalité de la demande d'autorisation préalable. Du point de vue technique et de la sécurisation des échanges, séparer l'authentification de la confidentialité est artificiel.

74. Dans la directive, les deux aspects sont liés. Ainsi, les PSC doivent : « *utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument ; »* ou encore «*prendre des mesures contre la contrefaçon des certificats, et dans les cas où le PSC génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données* » (annexe II, points f et g). De même, la fonction d'autorité de certification est liée à la technique de la cryptographie asymétrique. Or, dans ce procédé, authentification et confidentialité sont liées sur le plan fonctionnel.

75. Le projet de directive indique que les états membres doivent veiller à ce que les produits de signature électronique conformes à la directive puissent circuler librement sur le marché intérieur. Il s'agit d'un rappel du principe de libre circulation. Un produit de signature électronique librement commercialisé dans un autre pays de l'Union européenne doit pouvoir être fourni en France sans entrave. Surtout, les états membres ne doivent soumettre la fourniture des services de certification à aucune autorisation préalable (article 3.1).

76. On peut se demander si le fait que le décret n°99-199 du 17 mars 1999 substitue la formalité de la déclaration à celle de l'autorisation pour la fourniture de produits de cryptographie mis en

---

46[46] JO du 27 juillet 1996 ; décrets n° 98-101 et n° 98-102 du 24 février 1998.

47[47] Voir sur cette question : Valérie Sédallian, « Les problèmes posés par la législation française en matière de chiffrement », *Revue Droit de l'informatique et des télécoms*, 1998/4 p. 23.

48[48] JO du 19 mars 1999.

œuvre par un algorithme dont la clé est inférieure ou égale à 128 bits est suffisant au regard des exigences de la directive.

77. Les décrets d'application de la loi du 13 mars 2000 doivent mettre en œuvre les dispositions de la directive sur la signature électronique. Or, les prestataires de services de certification sont incontestablement des fournisseurs de services de cryptologie au sens de la loi du 26 juillet 1996. Est-il vraiment cohérent de transposer la directive sur les signatures électroniques sans avoir mis en œuvre, au préalable, la refonte annoncée de la législation relative à la cryptologie ?

Conclusion

78. Les prestataires de services de certification vont devenir de véritables agents de la preuve. A côté des services de signature électronique proprement dits, ils devront proposer également des services d'horodatage et d'archivage, deux questions étroitement liées à la preuve des actes juridiques, voire même des services de sécurité.

79. L'apparition d'un tiers certificateur dans la relation contractuelle afin d'assurer la preuve de l'acte conclu par voie électronique n'est pas sans rappeler l'acte authentique. La loi du 13 mars 2000 ne fait aucune référence à l'intervention des prestataires de services de certification qui interviennent dans le processus de signature électronique et dont le rôle est pourtant fondamental. La question se pose de savoir s'il n'aurait pas fallu les mentionner dans le texte de la loi49[49]50.

80. La signature, fonction personnelle51[50], reflet de la personnalité, va se trouver dépersonnalisée et déléguée à un système informatique géré par un tiers, dans lequel l'utilisateur devra avoir toute confiance. L'intervention d'un tiers dans le processus de signature est un changement radical, dont toutes les conséquences non plus juridiques, mais sociologiques, n'ont pas encore été mesurées.

V.S.

Notes

Voir également sur Juriscom.net :

- L'échange des consentements dans le commerce électronique
(Travaux Universitaires - Doctrine), de Lionel Thoumyre ;
- La nouvelle loi belge sur le commerce électronique
(Espace "Professionnels"), de Thibault Verbiest.

49[49] En ce sens, voir Rapport du groupe ad hoc signature électronique de IALTA France & Edifrance, 21 février 2000.

51[50] Souvenons-nous que le premier but d'un enfant qui apprend à écrire est d'être capable de tracer les signes composant son prénom…