

N° 203

SÉNAT

SESSION ORDINAIRE DE 1999-2000

Annexe au procès-verbal de la séance du 2 février 2000

RAPPORT

FAIT

au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur :

- *le projet de loi portant adaptation du **droit de la preuve** aux technologies de l'information et relatif à la **signature électronique** ;*

- *la proposition de loi de MM. Louis SOUVET, Louis ALTHAPÉ, Pierre ANDRÉ, Paul BLANC, Jean BERNARD, Louis de BROISSIA, Robert CALMEJANE, Auguste CAZALET, Charles de CUTTOLI, Xavier DARCOS, Désiré DEBAVELAERE, Luc DEJOIE, Jacques DELONG, Robert DEL PICCHIA, Charles DESCOURS, Michel ESNEU, Bernard FOURNIER, Yann GAILLARD, Patrice GÉLARD, Alain GÉRARD, Charles GINÉSY, Daniel GOULET, Alain GOURNAC, Georges GRUILLOT, Hubert HAENEL, Jean-Paul HUGOT, Roger HUSSON, André JOURDAIN, Christian de LA MALÈNE, Lucien LANIER, Robert LAUFOAULU, Guy LEMAIRE, Paul NATALI, Mme Nelly OLIN, MM. Jacques OUDIN, Jacques PEYRAT, Jean-Pierre SCHOSTECK, Jacques VALADE et Guy VISSAC visant à valider l'évolution jurisprudentielle en matière de **preuve par écrit** ;*

- *la proposition de loi de MM. Louis SOUVET, Louis ALTHAPÉ, Pierre ANDRÉ, Paul BLANC, Mme Paulette BRISEPIERRE, MM. Louis de BROISSIA, Robert CALMEJANE, Auguste CAZALET, Xavier DARCOS, Désiré DEBAVELAERE, Luc DEJOIE, Jacques DELONG, Robert DEL PICCHIA, Charles DESCOURS, Yann GAILLARD, Patrice GÉLARD, Alain GÉRARD, Charles GINÉSY, Daniel GOULET, Alain GOURNAC, Georges GRUILLOT, Hubert HAENEL, Jean-Paul HUGOT, Roger HUSSON, André JOURDAIN, Christian de LA MALÈNE, Lucien LANIER, Robert LAUFOAULU, Jacques LEGENDRE, Guy LEMAIRE, Bernard MURAT, Paul NATALI, Mme Nelly OLIN, MM. Joseph OSTERMANN, Jacques OUDIN, Jacques PEYRAT, Jean-Jacques ROBERT, Jean-Pierre SCHOSTECK, Martial TAUGOURDEAU et René TRÉGOUËT visant à reconnaître **la valeur probatoire d'un message électronique** et de sa signature,*

Par M. Charles JOLIBOIS,
Sénateur.

(1) Cette commission est composée de : MM. Jacques Larché, président ; René-Georges Laurin, Mme Dinah Derycke, MM. Pierre Fauchon, Charles Jolibois, Georges Othily, Michel Duffour, vice-présidents ; Patrice Gélard, Jean-Pierre Schosteck, Jacques Mahéas, Jean-Jacques Hyst, secrétaires ; Nicolas About, Guy Allouche, Jean-Paul Amoudry, Robert Badinter, José Balareello, Jean-Pierre Bel, Christian Bonnet, Robert Bret, Guy-Pierre Cabanel, Charles Ceccaldi-Raynaud, Marcel Charmant, Raymond Courrière, Jean-Patrick Courtois, Luc Dejoie, Jean-Paul Delevoye, Gérard Deriot, Gaston Flosse, Yves Fréville, René Garrec, Paul Girod, Daniel Hoeffel, Jean-François Humbert, Pierre Jarlier, Lucien Lanier, Simon Loueckhote, François Marc, Bernard Murat, Jacques Peyrat, Jean-Claude Peyronnet, Henri de Richemont, Simon Sutour, Alex Türk, Maurice Ulrich.

Voir les numéros :

Sénat : 488, 244 et 246 (1998-1999).

Droit civil.

SOMMAIRE

	<u>Pages</u>
LES CONCLUSIONS DE LA COMMISSION	5
EXPOSÉ GÉNÉRAL	6
I. LA NÉCESSITÉ DE RÉFORMER LE DROIT EXISTANT	8
A. L'ARCHITECTURE ACTUELLE DU DROIT DE LA PREUVE EN MATIÈRE CIVILE : LA PLACE CENTRALE DE L'ÉCRIT SUR SUPPORT PAPIER	9
1. <i>L'essentiel du droit civil français relève d'un régime de preuve légale</i>	9
2. <i>Deux notions distinctes : recevabilité et force probante</i>	9
a) La recevabilité des différents moyens de preuve	9
b) Force probante reconnue à chacun des moyens de preuve	9
3. <i>La prédominance de la preuve littérale</i>	10
4. <i>L'assimilation de la preuve par écrit au support papier</i>	10
5. <i>La charge de la preuve</i>	10
B. LE DROIT EN VIGUEUR N'EST PAS ADAPTÉ AUX ÉCHANGES ÉLECTRONIQUES	11
1. <i>Les questions à résoudre</i>	11
a) Les incertitudes sur le statut juridique des messages électroniques.....	11
b) La signature d'un acte juridique n'est pas définie dans le code civil.....	12
2. <i>Le droit en vigueur envisage les documents électroniques sur un mode mineur</i>	12
a) En règle générale, l'écrit électronique n'est pas admis en mode de preuve	12
b) Les cas où l'écrit électronique constitue une preuve recevable	13
c) Le document électronique est un « commencement de preuve par écrit »	14
3. <i>Les réponses jurisprudentielles sont partielles</i>	14
C. LA CONTRAINTE DU DROIT COMMUNAUTAIRE	14
1. <i>La recommandation sur les échanges de données informatisées</i>	15
2. <i>La directive sur le commerce électronique</i>	15
a) La conclusion de contrats électroniques doit être facilitée.....	16
b) La directive proposée s'applique à la validité des contrats électroniques	16
3. <i>La directive sur les signatures électroniques</i>	17
a) La notion de « signature électronique avancée »	17
b) Stricte égalité entre signature manuscrite et signature électronique avancée	17
II. LE PROJET DE LOI ET LES DEUX PROPOSITIONS DE LOI TENDENT À ADAPTER LE DROIT DE LA PREUVE ET RECONNAÎTRE LA SIGNATURE ÉLECTRONIQUE	19
A. LES TRAVAUX PRÉPARATOIRES SOULIGNENT LA NÉCESSITÉ D'UNE RÉFORME LÉGISLATIVE	19
1. <i>Le Conseil d'Etat se prononce pour une égalité entre document électronique et document papier</i>	19
a) La nécessité d'une réforme législative	19
b) Reconnaître la valeur probatoire du message électronique authentifié par une signature électronique fiable.....	19
(1) - une signature électronique remplit les fonctions d'une signature dès lors qu'elle est fiable ;.....	19
2. <i>Le groupe de travail du GIP « Droit et Justice » est favorable à la supériorité de l'écrit papier sur l'écrit électronique</i>	20
B. LES SOLUTIONS ECARTÉES PAR LE PROJET DE LOI	20
1. <i>Pas d'extension de la liberté de la preuve</i>	20
2. <i>Pas de nouvelle exception à la preuve par écrit</i>	21
3. <i>Pas de hiérarchisation entre support électronique et support papier</i>	22

C. LES DEUX PROPOSITIONS DE LOI.....	23
1. <i>Recevabilité en mode de preuve et force probante des télécopies</i>	23
2. <i>Force probante d'un message électronique et signature électronique</i>	24
D. LE PROJET DE LOI RETIENT CINQ ORIENTATIONS	24
1. <i>La redéfinition de la preuve littérale indépendamment du support utilisé</i>	25
2. <i>La valeur juridique du document électronique est équivalente à celle de l'acte sous seing privé</i>	25
a) <i>La recevabilité en mode de preuve du document électronique</i>	25
b) <i>La force probante du document électronique est équivalente à celle de l'acte sous seing privé</i>	25
c) <i>La suppression des mentions manuscrites</i>	25
3. <i>Le règlement des conflits de preuve</i>	26
4. <i>Les conventions sur la preuve</i>	26
5. <i>La définition générale de la signature et la reconnaissance de la signature électronique</i>	26
a) <i>Une définition générale de la signature</i>	26
b) <i>La signature électronique</i>	26
III. LA POSITION DE VOTRE COMMISSION DES LOIS : ÉTENDRE LE CHAMP D'APPLICATION DU PROJET DE LOI AUX ACTES AUTHENTIQUES	27
A. BIEN MESURER LA PORTÉE DE LA STRICTE ÉGALITÉ ENTRE SUPPORT PAPIER ET SUPPORT ÉLECTRONIQUE	27
B. DISTINGUER ÉCRIT « AD VALIDITATEM » ET ÉCRIT « AD PROBATIONEM »	28
1. <i>La distinction entre valeur ad validitatem et valeur ad probationem d'un acte juridique</i>	28
a) <i>L'écrit requis « ad solemnitatem » ou « ad validitatem »</i>	28
b) <i>L'écrit requis « ad probationem »</i>	28
2. <i>Votre commission des Lois souhaite réserver la reconnaissance de l'écrit électronique aux écrits ad probationem</i>	28
C. INCLURE LES ACTES AUTHENTIQUES.....	29
D. NE PAS SOUS-ESTIMER LES ASPECTS RÉGLEMENTAIRES	30
EXAMEN DES ARTICLES	31
• Article 1^{er} (art. 1315-1, 1316, 1316-1 et 1316-2 du code civil) Subdivisions du code civil relatives à la preuve	31
• Paragraphe 1^{er} de la section première du chapitre VI du titre troisième du Livre troisième du code civil Dispositions générales relatives à la preuve par écrit	32
• Article 1316 du code civil Définition de la preuve littérale indépendamment de son support	32
• Article 1316-1 du code civil Admissibilité en mode de preuve de l'écrit électronique	33
• Article 1316-2 du code civil Règlement des conflits de preuve littérale Conventions sur la preuve	38
• Article additionnel après l'article 1^{er} (art. 1317-1 du code civil) Actes authentiques	39
• Article 2 (art. 1322-1 du code civil) Force probante équivalente à celle de l'acte sous seing privé	42
• Article 3 (art. 1322-2 du code civil) Définition de la signature et de la signature électronique	44
• Article 4 (art. 1326 du code civil) Mentions manuscrites	48
• Article 5 Application outre-mer	50
TABLEAU COMPARATIF	51
ANNEXE AU TABLEAU COMPARATIF	55

ANNEXES	56
ANNEXE 1 - ÉTUDE D'IMPACT	57
ANNEXE 2 - QU'EST-CE QUE LA SIGNATURE ÉLECTRONIQUE ?	58
ANNEXE 3 - LES « AMENDEMENTS ÉLECTRONIQUES »	63
ANNEXE 4 - LÉGISLATION COMPARÉE	67
ANNEXE 5 - LISTE DES PERSONNES ENTENDUES	102

LES CONCLUSIONS DE LA COMMISSION

Réunie le mercredi 2 février 2000, sous la présidence de M. Jacques Larché, président, la commission des Lois, sur le rapport de M. Charles Jolibois, a examiné en première lecture le projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique.

Elle y a joint l'examen de deux propositions de loi de M. Louis Souvet et plusieurs de ses collègues, visant à valider l'évolution jurisprudentielle en matière de preuve par écrit et à reconnaître la valeur probatoire d'un message électronique et de sa signature.

Le projet de loi modifie le code civil afin d'**admettre en mode de preuve les documents électroniques**, mais aussi de prévoir que, **sous conditions, leur force probante sera équivalente à celle des documents sur support papier**. Pour ce faire :

- il définit la **preuve par écrit** de manière suffisamment générale pour inclure aussi bien les écrits sur support papier que sur support électronique ;

- il confie au juge le soin de régler les **conflits de preuve**, par exemple les cas où un écrit électronique et un écrit papier seraient contradictoires ;

- il supprime l'exigence de **mentions manuscrites** pour les actes unilatéraux ;

- il propose enfin une définition de la signature qui englobe aussi bien la signature manuscrite que la **signature électronique**, laquelle sera présumée fiable selon des modalités fixées par décret en Conseil d'Etat.

Outre deux amendements rédactionnels, la commission a adopté **trois amendements** tendant à :

- admettre la recevabilité en mode de preuve des **actes authentiques** établis et conservés sur support électronique (**article additionnel après l'article 1^{er}**);

- définir la signature électronique de l'officier public (**article 3**) ;

- préciser que la force probante des actes établis sur support électronique est subordonnée à des conditions de validité (**article 2**).

Elle a de plus souhaité **interroger le Gouvernement sur la suppression des mentions manuscrites en matière d'actes sous seing privé unilatéraux (article 4)**.

En conséquence, la commission des Lois a considéré que les deux propositions de loi soumises à son examen étaient satisfaites par le projet de loi.

Mesdames, Messieurs,

Le Sénat est appelé à examiner en première lecture le projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique.

Il est de plus saisi de deux propositions de loi présentées par M. Louis Souvet et plusieurs de ses collègues :

- la proposition de loi n° 244 (Sénat, 1998-1999) visant à valider l'évolution jurisprudentielle en matière de preuve par écrit,

- la proposition de loi n° 246 (Sénat, 1998-1999) visant à reconnaître la valeur probatoire d'un message électronique et de sa signature.

Votre rapporteur se félicite que ce projet de loi, adopté en Conseil des ministres le 1^{er} septembre 1999, ait été déposé en premier lieu sur le bureau du Sénat.

L'intérêt du Sénat pour les technologies de l'information s'est manifesté par la publication de plusieurs rapports, en particulier quatre rapports de l'Office parlementaire des choix scientifiques et technologiques :

- le rapport de M. Pierre Laffitte sur « *La France dans la société de l'information : un cri d'alarme et une croisade nécessaire* »¹, publié en février 1997 ;

- celui de M. Franck Sérusclat sur « *Les nouvelles techniques d'information et de communication : de l'élève au citoyen* »², publié en juin 1997 ;

- celui de M. Claude Huriet intitulé : « *Images de synthèse et monde virtuel : techniques et enjeux de société* »³, publié en décembre 1997 ;

- enfin le rapport intitulé : « *La société de l'information : quel avenir ?* »¹, publié en octobre 1997.

¹ Rapport n° 213 (Sénat, 1996-1997).

² Rapport n° 383 (Sénat, 1996-1997).

³ Rapport n° 169 (Sénat, 1997-1998).

Indépendamment des travaux de l'Office, doivent être notés :

- le rapport de MM. Alain Joyandet, Alex Türk et Pierre Hérisson, au nom de la mission commune d'information du Sénat sur l'entrée de la France dans la société de l'information, intitulé : « *Maîtriser la société de l'information : quelle stratégie pour la France ?* »², publié en septembre 1997 ;

- le rapport d'information de M. René Trégouët intitulé « *Des pyramides du pouvoir aux réseaux de savoirs* »³, publié en mars 1998 ;

- la proposition de loi⁴ de MM. Pierre Laffitte, René Trégouët et Guy Cabanel, tendant à généraliser dans l'administration l'usage d'Internet et de logiciels libres ;

- l'organisation au Sénat le 21 octobre 1999 d'un colloque de l'Association pour le développement de l'informatique juridique (ADIJ), présidé par votre rapporteur, ayant pour sujet : « *Quelle valeur probatoire accorder aux documents électroniques ?* ».

Cependant, hormis le cas de la dématérialisation de la facture autorisée par la « loi Madelin »⁵ du 11 février 1994, **le Parlement a rarement eu l'occasion de légiférer dans le domaine des technologies de l'information.**

Or, le développement du commerce électronique entraîne une **multiplication des documents électroniques échangés**. En 1998, le commerce électronique était estimé en France à 800 milliards de francs pour les échanges de données informatisées, deux milliards de francs pour le commerce interentreprises sur Internet et de 500 millions à un milliard de francs pour le commerce électronique sur Internet en direction des particuliers.

De plus, le commerce dit « en ligne », qui désigne la fourniture des biens et des services commandés sur le réseau⁶, implique que **la passation du contrat de vente mais aussi son exécution revêtent une forme électronique**. L'ordre de paiement doit donc être émis directement sur Internet.

Dès lors, se pose la question de la recevabilité des écrits informatiques pour **prouver le contenu d'un contrat électronique**. Force est de constater que l'état actuel du droit ne reconnaît la recevabilité des documents électroniques en mode de preuve qu'au cas par cas, à l'appréciation des juges du fond. De plus, le droit en vigueur ne confère pas aux écrits électroniques la même force probante qu'aux écrits sur support papier.

¹ Actes de la journée d'étude du 9 octobre 1997.

² Rapport n° 436 (Sénat, 1996-1997).

³ Rapport n° 331 (Sénat, 1997-1998).

⁴ Proposition de loi n° 117 (Sénat, 1999-2000).

⁵ Loi n° 94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle, article 4.

⁶ Par exemple le téléchargement du logiciel commandé ou la transmission des informations d'une banque de données.

L'intervention du législateur paraît aujourd'hui nécessaire pour faire entrer « par la grande porte » les écrits électroniques dans le code civil. Cette réforme législative est d'autant plus significative que les dispositions du code civil relatives à la preuve avaient très peu été modifiées depuis l'adoption du « code Napoléon ».

Le présent projet de loi propose d'admettre en mode de preuve les documents électroniques, mais aussi de prévoir que, sous conditions, leur force probante sera équivalente à celle des documents sur support papier.

Le projet de loi propose plusieurs moyens pour ce faire : il définit la preuve par écrit de manière suffisamment générale pour inclure aussi bien les écrits sur support papier que sur support électronique ; il confie au juge le soin de régler les conflits de preuve, par exemple les cas où un écrit électronique et un écrit papier seraient contradictoires ; il supprime l'exigence de mentions manuscrites pour les actes unilatéraux ; il propose enfin une définition de la signature qui englobe aussi bien la signature manuscrite que la **signature électronique**.

Il part ainsi du principe que **la même confiance peut être accordée à une signature électronique qu'à une signature manuscrite**, toutes deux servant à manifester le **consentement** du signataire au contenu de l'acte.

Pour que cette confiance soit établie, des prescriptions fixées par décret détermineront la fiabilité des techniques employées. La signature électronique est créée par des logiciels spécifiques, permettant à l'émetteur de **sceller** son document et éventuellement de le **crypter** ; le destinataire et l'émetteur détiennent des « **clés** » (gérées par le logiciel spécifique de création de signature) qui garantissent la **confidentialité** des messages ainsi échangés¹.

*

Après avoir constaté les lacunes du droit actuellement en vigueur, et examiné les orientations du projet de loi et des deux propositions de loi, la commission des Lois a décidé de modifier le champ d'application du projet de loi afin de reconnaître l'acte authentique électronique.

LA NÉCESSITÉ DE RÉFORMER LE DROIT EXISTANT

Après avoir examiné les grandes lignes du droit de la preuve français, puis la façon dont le droit en vigueur envisage les documents électroniques, votre commission a constaté que les solutions actuelles constituent un frein au développement des échanges « en ligne ».

¹ Voir en annexe la description des aspects techniques de la signature électronique.

L'ARCHITECTURE ACTUELLE DU DROIT DE LA PREUVE EN MATIÈRE CIVILE : LA PLACE CENTRALE DE L'ÉCRIT SUR SUPPORT PAPIER

En matière juridique, la preuve désigne le moyen par lequel on pourra, ou on aura le droit, d'établir l'exactitude de ce qu'on allègue : écrits témoignages, aveu... En droit civil, les règles de preuve sont fixées par la loi et accordent une prééminence à l'écrit, entendu comme écrit sur support papier.

L'essentiel du droit civil français relève d'un régime de preuve légale

Le **régime de la preuve libre** désigne la capacité pour les parties de présenter toute forme de preuve à l'appui de leur demande. Il n'existe ainsi aucune hiérarchie entre les modes de preuve, cette question étant laissée à l'appréciation souveraine des juges du fond. Les documents électroniques sont donc admis en mode de preuve dans tous les cas où le droit français prévoit expressément que la preuve est librement apportée par les parties.

Ce régime est applicable en France en droit pénal (système de l'intime conviction), en droit administratif, en droit commercial (sauf la preuve du commerçant contre le consommateur) et pour une partie importante du droit civil (actes juridiques n'excédant pas le seuil de 5.000 francs).

Au contraire, dans le **régime de la preuve légale**, la loi impose au juge et aux parties certains procédés de preuve. Le droit civil distingue la preuve des **faits**, qui relève de l'intime conviction du juge, de la preuve des **actes juridiques**, pour lesquels le principe est posé qu'un acte juridique ne peut se prouver que par écrit. La **préconstitution d'un document écrit**, signé, est ainsi souvent requise par la loi.

Dans un système de preuve légale, le législateur doit intervenir pour admettre la recevabilité de nouveaux modes de preuve ou redéfinir les moyens de preuve existants. A défaut de cette intervention, l'admission des documents électroniques est problématique.

Deux notions distinctes : recevabilité et force probante

La recevabilité des différents moyens de preuve

La loi établit quels moyens sont **recevables** en mode de preuve, c'est-à-dire les **moyens par lesquels une partie a le droit d'établir l'exactitude de ce qu'elle allègue**. Le droit civil reconnaît cinq modes de preuve : par écrit, par témoignage, par présomption, par aveu de la partie et par serment.

Force probante reconnue à chacun des moyens de preuve

A la question de la recevabilité s'ajoute celle de la **force probante** d'un document. Parmi les différents moyens de preuve présentés par les

emportera la conviction du juge. Le régime français de la preuve légale établit entre les différents modes de preuve une véritable hiérarchie. Ce n'est que dans le cas où la loi ne détermine pas le degré de force probante d'un mode de

La prédominance de la preuve littérale

Au sommet de cette hiérarchie se trouve l'écrit

ceux sous forme d'acte authentique (le plus souvent un acte notarié) ou d'acte sous seing privé, c'est-à-dire signé des parties.

considérés comme ayant une force probante. Par exemple, un contrat qui ne peut pas être prouvé, faute d'écrit, sans être nul au sens juridique du mot, n'a pas de force probante ; sauf si la personne a la possibilité de produire une autre preuve équivalente à l'écrit, tel

L'assimilation de la preuve par écrit au support papier

L'assimilation de la preuve par écrit imposée dans de nombreux domaines, repose sur le principe de la hiérarchie des modes de preuve, en particulier les témoignages.

contenu et son support :

papier¹

était le seul support utilisé pour constater l'existence et le contenu des contrats et en faire la preuve.

Celui qui réclame l'exécution d'une obligation doit la prouver. Réciproquement, celui qui se prétend libéré, doit justifier le paiement ou le fait

Le problème de la charge de la preuve

d'obligations contractuelles, peut se poser aux différents stades du contrat :

¹

admet la production d'écrits sur du sable, de la pierre, une ardoise... A titre d'exemple, un testament peut être écrit sur le dessus et le côté d'une machine à laver (Nancy, 26 juin 1986), tracés.

- la naissance de l'obligation, liée à la formation du contrat (prouver l'existence du contrat et du consentement) ;

- la nature ou qualification du contrat (par exemple distinguer prêt et donation, vente et donation déguisée) ;

- les modalités du contrat ; l'extinction de l'obligation, par le paiement ou un autre mode d'extinction ;

- l'inexécution du contrat et la responsabilité contractuelle.

La partie sur laquelle repose la charge de la preuve a tout intérêt à se **préconstituer une preuve** si elle souhaite réduire le risque de preuve qui pèse sur elle.

LE DROIT EN VIGUEUR N'EST PAS ADAPTÉ AUX ÉCHANGES ÉLECTRONIQUES

L'intervention du législateur est d'autant plus nécessaire que le droit actuellement applicable est source d'incertitudes sur la valeur probante des documents électroniques.

Les questions à résoudre

Les incertitudes sur le statut juridique des messages électroniques

Comme le souligne le Conseil d'Etat¹, « ***le fait qu'un message électronique puisse, en l'état actuel des textes, être assimilable à l'un des écrits visés à l'article 1341 du code civil² demeure très contesté*** ».

De multiples interrogations sur le **statut juridique des messages électroniques** freinent l'essor des échanges en ligne :

- lorsque la loi exige un écrit, les messages électroniques satisfont-ils à cette obligation ?

- ces messages sont-ils dotés d'une valeur probante ?

- une signature électronique peut-elle conférer à un message électronique une valeur juridique ?

¹ Rapport « Internet et les réseaux juridiques ».

² L'article 1341 du code civil pose le principe de l'obligation d'un écrit en matière civile pour tous engagements supérieurs à 5.000 francs, et l'impossibilité de prouver par témoignage contre un écrit préconstitué.

La signature d'un acte juridique n'est pas définie dans le code civil

Alors que de nombreux actes juridiques comportent comme condition de leur validité la signature de la partie à laquelle l'acte est opposé, le code civil ne définit pas la signature. Cependant, il existe un consensus sur les fonctions de la signature. Ainsi, la **signature** apposée sur un document est susceptible d'emporter **trois types d'effets** :

- l'expression par l'auteur de l'acte de son consentement ;
- l'établissement de la preuve de cet acte juridique en cas de contestation (valeur juridique *ad probationem*)¹ ;
- le respect, le cas échéant, d'un formalisme conditionnant la validité de l'acte (valeur juridique *ad validitatem*)².

Le droit en vigueur envisage les documents électroniques sur un mode mineur

Jusqu'à présent, l'écrit électronique ne constitue qu'un élément de preuve, un indice, une présomption. Il n'est admis en mode de preuve que dans des conditions strictement définies.

En règle générale, l'écrit électronique n'est pas admis en mode de preuve

Il est à l'heure actuelle impossible de recourir aux messages électroniques s'agissant des actes pour lesquels, en application de l'**article 1341** du code civil³, la preuve par écrit est exigée, ou pour lesquels la loi impose des conditions de recevabilité et de force probante :

- engagements supérieurs à 5.000 francs ;

¹ *L'écrit peut être exigé ad probationem, ce qui signifie que l'écrit n'est pas demandé comme élément nécessaire à la perfection du contrat, mais uniquement pour en établir la réalité et la teneur. Il vaut « pour la preuve ». S'il fait défaut, il n'y a pas pour autant inexistence juridique de l'acte, mais simplement difficultés d'en justifier. Par exemple, dans le cas des écrits qui doivent être établis en double exemplaire, parce qu'ils font naître des obligations à la charge de chaque partie (on peut citer le cas des **contrats de bail**), l'inobservation de cette obligation n'entraîne pas la nullité de la convention elle-même mais prive seulement l'écrit de sa force probante.*

² *Il peut aussi être exigé ad validitatem : en l'absence d'écrit, l'opération est privée d'existence juridique, l'écrit étant requis « pour la solennité », c'est-à-dire qu'il est imposé pour la validité de l'acte. Par exemple, en matière de **prêt à intérêt**, l'exigence d'un écrit mentionnant le taux de l'intérêt conventionnel est une condition de validité de la stipulation d'intérêt.*

³ *L'article 1341 du code civil dispose : « Il doit être passé acte devant notaires ou sous signatures privées de toutes choses excédant une somme ou une valeur fixée par décret, même pour dépôts volontaires, et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse d'une somme ou valeur moindre.*

« Le tout sans préjudice de ce qui est prescrit dans les lois relatives au commerce. »

- actes sous seing privé ;
- actes authentiques ;
- actes devant être établis en double exemplaire (actes synallagmatiques, article 1325 du code civil) ;
- actes devant contenir des mentions spécifiques (article 1326).

Les cas où l'écrit électronique constitue une preuve recevable

La force probatoire de l'acte est subordonnée à sa forme et à son support. L'acte juridique exprimé par **un message électronique constitue une preuve recevable lorsque la loi n'exige aucun formalisme particulier.**

Il s'agit notamment des **relations commerciales**. L'article 109 du code de commerce¹ dispose qu'à l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens, à moins qu'il n'en soit autrement disposé par la loi. Il s'agit d'un régime de **liberté de la preuve**, c'est-à-dire que tous les modes de preuve sont admissibles en matière commerciale, y compris la preuve par présomption et la preuve par témoin. Par exemple, le juge peut retenir à titre de présomption simple la composition d'un code confidentiel d'un système informatique fonctionnant régulièrement.

En matière civile, des textes législatifs ou réglementaires ont créé des **dérogations** à l'assimilation de la preuve par écrit au support papier. **Sont ainsi recevables comme mode de preuve les documents électroniques :**

- lorsqu'ils constatent un engagement inférieur à 5.000 francs (article 1341 du code civil et décret du 15 juin 1980) ;
- lorsqu'il existe un commencement de preuve par écrit (article 1347 du code civil) ;
- lorsqu'existent des circonstances exceptionnelles, une impossibilité matérielle ou morale interdisant de préconstituer une preuve ou de rappeler un original (1^{er} alinéa de l'article 1348 du code civil) ;
- en matière de comptabilité² et de facture (loi du 11 février 1994 autorisant la dématérialisation de la facture) ;

Dans les cas énumérés ci-dessus, les messages électroniques sont admissibles comme preuve car ils sont considérés comme ayant la même valeur que les documents papiers originaux.

¹ L'article 109 ne vaut que pour la preuve des actes de commerce entre commerçants ou opposés à l'encontre d'un commerçant.

² Loi n°83-353 du 30 avril 1983 et décret n° 83-1020 du 29 novembre 1983 sur l'information de la comptabilité

Le document électronique est un « _____ »

L'acte sur support électronique ne vaut que comme

Le juge détermine la valeur du document électronique en se fondant sur la notion de « _____ » définie à l'article 1347¹ comme « *tout acte par écrit qui est émané de celui contre lequel la demande est formée, ou de celui qu'il représente, et le fait allégué* ».

La jurisprudence est rare en matière d'écrits électroniques.

Cependant, un arrêt très remarqué de la **Cour de cassation**, rendu le _____, Société Descamps contre Banque Scalbert Dupont, a affirmé qu'« *un acte peut être établi et conservé sur tout support, dès lors que son _____ et l'imputabilité l'auteur désigné ont été vérifiées, ou ne sont pas contestées* ».

que soit son support. Mais il ne s'agit pas d'une règle générale. Comme dans tous les contentieux de la preuve, les circonstances de l'espèce sont contenu n'était pas contesté, et portant sur une cession de créance professionnelle. Ces trois circonstances soulignent que cet arrêt de la Cour de électronique en mode de preuve.

*

la jurisprudence rendent nécessaire une intervention du législateur. Celui-ci est de plus contraint par les prescriptions du droit communautaire.

LA CONTRAINTE DU DROIT COMMUNAUTAIRE

De nombreux actes de l'Union européenne, dont la valeur contraignante est variable, traitent des documents sous forme électronique et de la signature électronique.

¹ L'article 1347 du code civil prévoit une double exception :
- exception à l'obligation définie à l'article 1341 d'une preuve préconstituée en matière civile au-delà de 5.000 francs,
- exception à l'interdiction de prouver par tous moyens contre et outre le contenu des écrits.
En d'autres termes, lorsqu'existe un commencement de preuve par écrit, c'est-à-dire lorsque l'écrit présenté ne suffit pas à établir complètement l'existence et le contenu de l'acte litigieux, la preuve testimoniale est recevable.

Votre rapporteur ne les citera pas tous, mais s'intéressera à trois d'entre eux qui limitent la marge de manœuvre du législateur national. Force est de constater que les décisions prises au niveau communautaire n'ont de « recommandation » et de « directives » que le nom, et qu'elles déterminent *dans le détail* le régime juridique applicable aux contrats sous forme électronique.

La recommandation sur les échanges de données informatisées

La Commission européenne a publié le 19 octobre 1994 une recommandation concernant les aspects juridiques de l'échange de données informatisées¹ (EDI), qui tend à généraliser l'usage de l'« accord type européen pour l'EDI » dans les relations commerciales entre acteurs économiques et organisations de l'Union européenne.

En application de l'article 4 de cette recommandation, dans la mesure où les lois nationales le permettent, les parties s'engagent à accepter, en cas de litige, que les enregistrements des messages EDI qui ont été conservés conformément aux dispositions de cet accord soient admissibles devant les tribunaux et **fassent preuve des faits qu'ils contiennent, à moins qu'une preuve contraire ne soit présentée.**

De plus, les parties s'engagent à mettre en œuvre et à maintenir des procédures et des mesures de sécurité afin d'assurer la protection des messages EDI contre les risques d'accès non autorisés, de modification, de retard, de destruction ou de perte. Les procédures et les mesures de sécurité comprennent la vérification de l'**origine** et de l'**intégrité**, la **non-répudiation** de l'origine et de la réception des messages EDI et leur **confidentialité**.

Cet accord type européen sur les EDI préfigure les deux objets du projet de loi soumis à votre examen : rendre compatible le droit de la preuve avec les nouvelles modalités d'établissement et de transmission des données, sécuriser ces échanges par des moyens technologiques adaptés. S'il n'est pas contraignant, il n'en va pas de même des deux propositions de directive communautaire qui l'ont suivi.

La directive sur le commerce électronique

La proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur² n'est pas encore définitive mais a fait l'objet d'un accord politique

¹ *L'échange de données informatisées (EDI) est le transfert électronique, d'un ordinateur à un autre, de données commerciales et administratives sous la forme d'un message EDI structuré conformément à une norme agréée.*

² *Voir le rapport n° 178 (Sénat, 1999-2000) de votre rapporteur au nom de la commission des Lois sur la proposition de résolution de la Délégation du Sénat pour l'Union européenne relative à cette proposition de directive.*

en Conseil de l'Union européenne, en formation « marché intérieur », le 7 décembre 1999.

La conclusion de contrats électroniques doit être facilitée

La directive proposée dispose dans son article 9, consacré au traitement des contrats par voie électronique, que « *les Etats membres veillent à ce que leur système juridique rende possibles les contrats par voie électronique* ».

Aux termes de la directive proposée, « *les Etats membres s'assurent notamment que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ou **ne conduise pas à priver d'effet et de validité juridique de tels contrats pour le motif qu'ils sont passés par voie électronique*** ».

Cependant, les Etats membres peuvent prévoir que les dispositions ci-dessus mentionnées ne s'appliquent pas aux contrats suivants :

- les contrats qui créent ou transfèrent des droits sur les biens immobiliers, à l'exception des droits de location ;

- les contrats pour lesquels la loi requiert l'intervention de tribunaux, d'autorités publiques ou de professions exerçant une autorité publique ;

- les contrats de caution et de garantie fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale ;

- les contrats relevant du droit de la famille ou du droit des successions.

La directive proposée s'applique à la validité des contrats électroniques

Cette directive, qui doit être transposée en droit national dans le délai de dix-huit mois suivant son entrée en vigueur, restreint considérablement les possibilités offertes au législateur national.

En effet, elle ne se contente pas de prescrire aux Etats membres de reconnaître les contrats électroniques selon les modalités qu'ils jugeront utiles d'adopter, conformément à l'objet d'une « directive », censée n'imposer de contraintes qu'en termes d'**objectifs**.

Au contraire, elle impose aux Quinze de garantir aux contrats électroniques « **effet et validité juridique** ». Cette disposition est précisée dans la directive spécialement consacrée aux signatures électroniques.

La directive sur les signatures électroniques

La directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques a été publiée au Journal Officiel des Communautés européennes le 19 janvier 1999.

L'**objectif** de cette directive est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Comme la directive sur le commerce électronique, elle s'attache avant tout à garantir le bon fonctionnement du marché intérieur.

Elle ne couvre pas les aspects liés à la conclusion et à 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^{er}).

La notion de « signature électronique avancée »

La directive définit les nombreuses notions nouvelles introduites dans le droit applicable (article 2).

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 ».

La directive introduit la notion de « **signature électronique avancée** » qui est celle que transpose le projet de loi soumis à votre examen. La signature électronique est *avancée* lorsqu'elle satisfait aux 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**¹.

Stricte égalité entre signature manuscrite et signature électronique avancée

L'article 5 de la directive est consacrée aux **effets juridiques** des signatures électroniques : les Etats membres veillent à ce que les signatures électroniques avancées fondées sur un « certificat qualifié » et créées par un dispositif sécurisé de création de signature :

¹ Voir en annexe les modalités techniques de la signature électronique.

- d'une signature à l'égard de données électroniques répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier **non-discrimination** ;

et soient recevables comme preuves en justice .

De nombreuses dispositions de la directive s'appliquent aux réglementaire.

Cette directive doit être transposée en droit national dans le délai de suivant son entrée en vigueur. Force est de constater l'avance prise par la France en la matière, puisque le présent projet de loi a été adopté^{er} septembre 1999 alors que la directive qu'il

En vertu de cette directive, la signature électronique répondant à certaines exigences techniques sera automatiquement réputée de même valeur judiciaires.

Votre commission des Lois ne peut que constater la solution ainsi juridique d'un document électronique pourrait se voir opposer le non-respect du droit communautaire.

électronique avancée ne va pas de soi (voir *infra* solutions auraient pu être apportées, dans la mesure où le droit français de la preuve en matière civile offre des nuances souvent protectrices, dans le objectif constant du législateur.

*

directive communautaire qu'il est chargé de transposer.

¹ De plus, les preuve en justice ne soient pas refusées à une signature électronique au seul motif que : la signature se présente sous forme électronique,

- ou qu'elle ne repose pas s service de certification,

-

LE PROJET DE LOI ET LES DEUX PROPOSITIONS DE LOI TENDENT À ADAPTER LE DROIT DE LA PREUVE ET RECONNAÎTRE LA SIGNATURE ÉLECTRONIQUE

LES TRAVAUX PRÉPARATOIRES SOULIGNENT LA NÉCESSITÉ D'UNE RÉFORME LÉGISLATIVE

Le Conseil d'Etat se prononce pour une égalité entre document électronique et document papier

La section du rapport et des études du Conseil d'Etat a publié un rapport intitulé : « Internet et les réseaux numériques », adopté par l'Assemblée générale du Conseil d'Etat en juillet 1998. Une partie de ce rapport est consacrée à la reconnaissance de la valeur juridique du document et de la signature électroniques.

La nécessité d'une réforme législative

Le Conseil d'Etat rappelle que le législateur a déjà admis ponctuellement qu'un message électronique tienne lieu d'écrit¹. Il ajoute qu'une reconnaissance rapide de la valeur juridique du document électronique s'impose et rend nécessaire une adaptation du code civil.

Reconnaître la valeur probatoire du message électronique authentifié par une signature électronique fiable

Le résumé des propositions du Conseil d'Etat tient en cinq points :

- une signature électronique remplit les fonctions d'une signature dès lors qu'elle est fiable ;

- lorsqu'un document électronique assorti d'une signature électronique est présenté pour établir la preuve d'un acte, il ne saurait être contesté au seul motif qu'il se présente sous forme électronique ;

- **le document électronique tient lieu d'acte sous seing privé** dès lors qu'il est assorti d'une signature fiable et qu'il est conservé avec celle-ci de façon durable ;

¹ Il s'agit de la dématérialisation des factures prévue à l'article 47 de la loi de finances pour 1990 (« Les factures transmises par voie télématique constituent des documents tenant lieu de factures d'origine ») ou de la transmission par voie électronique d'une déclaration administrative (article 4 de la loi du 11 février 1994). La mise en œuvre d'une déclaration par voie électronique doit respecter certaines exigences tenant à l'identification de l'auteur de l'acte, à l'intégrité et à la fiabilité de la transmission, à l'horodation, à l'accusé de réception et à la conservation du message.

- si le document électronique est accompagné d'un certificat répondant à certaines exigences, délivré par une autorité de certification accréditée, la fiabilité de la signature et la conservation durable du document signé sont présumées ;

- dans le cas inverse, il appartiendra à celui qui entend se prévaloir d'un document électronique signé mais non certifié de démontrer que les conditions de fiabilité et de conservation sont remplies.

Le groupe de travail du GIP « Droit et Justice » est favorable à la supériorité de l'écrit papier sur l'écrit électronique

La mission de recherche « Droit et Justice », constituée sous forme de groupement d'intérêt public, a constitué un comité d'experts sur le thème de « **L'écrit et les nouveaux moyens technologiques au regard du droit** », qui a remis un rapport en septembre 1997.

Le comité d'experts souligne tout d'abord que la **préconstitution de preuve doit être conservée parce qu'elle garantit l'égalité des parties devant le risque de la preuve** et parce que c'est le système dont la légitimité s'impose le plus facilement au juge.

Le comité d'experts propose une définition de la preuve par écrit, ou preuve littérale, qui ne dépende ni du support utilisé, ni des modalités du transfert.

Il propose de reconnaître explicitement le statut des écrits électroniques comme mode de preuve, à condition que soit dûment identifiée la personne dont émane le document électronique et que celui-ci ait été établi et soit conservé de manière fiable.

LES SOLUTIONS ECARTÉES PAR LE PROJET DE LOI

Pas d'extension de la liberté de la preuve

L'élargissement du régime de la preuve libre a été écarté :

- le projet de loi ne propose pas d'élargir le champ de l'article 109 du code de commerce (preuve libre entre commerçants) aux actes mixtes, c'est-à-dire l'acte mettant en présence deux parties dont l'une seulement est commerçante ou l'acte qui n'est commercial que pour l'une des parties ;

- il ne revient pas sur les articles 1345 et 1346 du code civil¹ qui considèrent la demande en justice et non le montant unitaire de l'opération pour le calcul du montant des 5.000 francs ;

- enfin, il ne propose pas le relèvement du seuil de 5.000 francs dans la mesure où celui-ci est fixé par voie réglementaire.

Il n'a pas paru souhaitable de restreindre à l'excès le champ d'application du régime de la preuve légale. Le Conseil d'Etat a jugé « radicale » l'option consistant à instaurer en France un régime de liberté de la preuve ou à réévaluer très nettement le seuil prévu à l'article 1341 du code civil.

Au contraire, le régime de preuve légale, en particulier l'obligation pour les commerçants de respecter les dispositions de l'article 1341 du code civil relatives à **la préconstitution de preuve par écrit, est de nature à protéger les consommateurs.**

Pas de nouvelle exception à la preuve par écrit

L'article 1348 du code civil² prévoit des exceptions à l'exigence d'un écrit posée par l'article 1341, en cas d'**impossibilité d'établir un écrit**. Les juges du fond apprécient souverainement si une partie s'est trouvée dans l'impossibilité de produire une preuve littérale.

Il existe des **divergences d'appréciation sur la question des exceptions à la preuve littérale.**

Le Conseil national du crédit et du titre (CNCT), dans un rapport consacré aux « *Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres* » (mai 1997), s'est prononcé en faveur d'une modification de l'article 1348 du code civil, afin que l'exigence d'un écrit reçoive exception lorsque le titre est établi et conservé sous forme électronique dans des conditions assurant son intégrité et permettant l'imputabilité à son auteur.

De même, certains proposent de faire du recours à l'informatique un cas de dispense systématique du premier alinéa de l'article 1348 du code civil,

¹ Selon l'article 1345 du code civil, « si, dans la même instance, une partie fait plusieurs demandes, dont il n'y ait point de titre par écrit, et que, jointes ensemble, elles excèdent la somme prévue à l'article 1341, la preuve par témoin n'en peut être admise... ».

² L'article 1348 du code civil dispose : « Les règles ci-dessus reçoivent encore exception lorsque l'obligation est née d'un quasi-contrat, d'un délit ou d'un quasi-délit, ou lorsque l'une des parties, soit n'a pas eu la possibilité matérielle ou morale de se procurer une preuve littérale de l'acte juridique, soit a perdu le titre qui lui servait de preuve littérale, par suite d'un cas fortuit ou d'une force majeure.

« Elles reçoivent aussi exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support ».

en ajoutant à l'impossibilité matérielle et morale l'impossibilité technique. Cette solution présenterait l'inconvénient de faire de l'écrit informatique un mode de preuve imparfait, en tant qu'exception à l'article 1341.

Le projet de loi n'a pas retenu la proposition tendant à ranger le message électronique dans la catégorie du **commencement de preuve par écrit (article 1347 du code civil)**. En effet, il ne s'agirait que d'un début de preuve qui devrait être complété par d'autres éléments extrinsèques à l'acte (par exemple un témoignage) ; de plus, le commencement de preuve doit émaner de celui contre lequel la demande est formée. Dans ces conditions, il paraît difficile d'apporter des éléments de preuve dans un contexte d'échanges informatiques.

Le projet de loi écarte la solution tendant à intégrer le document électronique dans les dérogations ouvertes par le premier alinéa de l'**article 1348** du code civil, relatif aux cas d'**impossibilité de se procurer un écrit**, en ajoutant l'impossibilité technique. En effet, il n'est jamais impossible techniquement d'accompagner un échange électronique par un contrat écrit. Or, l'esprit de l'article 1348 consiste à réserver la dérogation à un fait exceptionnel, auquel il paraît difficile d'assimiler l'état de la technique.

Enfin, le projet de loi n'a pas rangé les documents électroniques dans le champ des exceptions à l'écrit posées par le second alinéa de l'article 1348, ce qui reviendrait à les assimiler à des copies constituant une **reproduction fidèle et durable**, dans la mesure où la logique de la copie, qui suppose l'existence d'un original, se prête mal à l'informatique.

Pas de hiérarchisation entre support électronique et support papier

De nombreux débats ont eu lieu autour de la question de **l'établissement dans la loi d'une hiérarchie des preuves en cas de contradiction entre un écrit sur support papier et un écrit électronique**.

Le GIP « Droit et Justice », avec prudence, a considéré qu'il était nécessaire de maintenir une hiérarchie entre l'écrit sur support papier et l'écrit électronique, dans les cas où l'écrit sur support papier était authentifié, c'est-à-dire signé des parties.

Il lui a paru utile de prévoir dans la loi qu'*« il ne peut être prouvé par un écrit électronique outre et contre un acte rédigé sur des registres ou papiers quelconques et signé des parties »*.

De plus, s'interrogeant sur la force probante de l'écrit électronique quand celui-ci n'est pas opposé à un écrit sur support papier, le comité d'experts a décidé de rappeler le principe selon lequel la preuve contraire ne

peut être admise que sur le fondement de présomptions graves, précises et concordantes¹.

Cette rédaction tendrait à reconnaître un poids certain à la force probante de l'écrit électronique, **qui ne peut être remise en cause que par des présomptions graves, précises et concordantes**, l'appréciation des présomptions étant laissée à l'intime conviction du juge.

Le code civil québécois va plus loin, en prévoyant que les inscriptions informatisées peuvent être contredites **par tous moyens**, c'est-à-dire que l'écrit électronique peut être contesté par tout mode de preuve, en particulier par témoin.

Cependant, cette hiérarchisation entre les supports de preuve littérale n'a pas été retenue par le projet de loi (voir *infra*).

LES DEUX PROPOSITIONS DE LOI

Deux propositions de loi ont été jointes à l'examen du projet de loi gouvernemental, toutes deux présentées par M. Louis Souvet et plusieurs de ses collègues en mars 1999.

Recevabilité en mode de preuve et force probante des télécopies

La proposition n° 244² (Sénat, 1998-1999) vise à inscrire dans la loi les évolutions jurisprudentielles en matière de preuve par écrit. Elle un objet limité, puisqu'elle tend à reconnaître la valeur probatoire des seules **télécopies**. Elle introduit toutefois deux notions essentielles, tenant à l'intégrité du document transmis par voie télématique et à l'imputabilité de ce document à son auteur.

Elle tend à compléter l'article 1334 du code civil³ : « *Les télécopies font foi entre les parties, sous réserve, en cas de doute, d'un examen*

¹ L'article 1353 du code civil dispose : « *Les présomptions qui ne sont point établies par la loi sont abandonnées aux lumières et à la prudence du magistrat, qui ne doit admettre que des présomptions graves, précises et concordantes, et dans les cas seulement où la loi admet les preuves testimoniales, à moins que l'acte ne soit attaqué pour cause de fraude ou de dol* ».

² Cette proposition de loi est présentée par MM. Louis Souvet, Louis Althapé, Pierre André, Paul Blanc, Jean Bernard, Louis de Broissia, Robert Calmejane, Auguste Cazalet, Charles de Cuttoli, Xavier Darcos, Désiré Debavelaere, Luc Dejoie, Jacques Delong, Robert Del Picchia, Charles Descours, Michel Esneu, Bernard Fournier, Yann Gaillard, Patrice Gélard, Alain Gérard, Charles Ginésy, Daniel Goulet, Alain Gournac, Georges Gruillot, Hubert Haenel, Jean-Paul Hugot, Roger Husson, André Jourdain, Christian de La Malène, Lucien Lanier, Robert Laufoaulu, Guy Lemaire, Paul Natali, Mme Nelly Olin, MM. Jacques Oudin, Jacques Peyrat, Jean-Pierre Schosteck, Jacques Valade et Guy Vissac, sénateurs.

³ Actuellement, l'article 1334 du code civil dispose que « *les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la présentation peut toujours être exigée* ».

approfondi permettant d'éliminer les pièces douteuses quant à leur intégrité et à l'imputabilité de leurs contenus ».

Force probante d'un message électronique et signature électronique

Dans l'objectif de favoriser le développement du commerce électronique, en l'entourant de précautions afin d'éviter les abus de confiance et escroqueries, la proposition de loi n° 246 (Sénat, 1998-1999) vise à reconnaître la valeur probatoire d'un message électronique et de sa signature¹.

Elle tend à reconnaître la valeur probatoire d'un message électronique et le rôle de la signature électronique fiable pour authentifier l'auteur de l'acte. Elle insiste de plus sur le rôle du juge et sur les impératifs de conservation durable des documents ainsi échangés.

La valeur probatoire d'un document électronique serait subordonnée à deux conditions cumulatives :

- « *d'une part, que soit possible l'**authentification** par une signature électronique **fiable** » ;*

- « *d'autre part, que soit assurée la **conservation** durable du message sous le contrôle du signataire ».*

Votre commission montrera que ces deux propositions de loi sont satisfaites par le texte proposé par le Gouvernement.

LE PROJET DE LOI RETIENT CINQ ORIENTATIONS

Le projet de loi soumis à votre examen s'inspire largement des travaux du Conseil d'Etat et de ceux de la Mission pour le commerce électronique². Il ne retient que certaines propositions du comité d'experts du GIP « Droit et Justice ».

¹ Cette proposition de loi est présentée par MM. Louis Souvet, Louis Althapé, Pierre André, Paul Blanc, Mme Paulette Brisepierre, MM. Louis de Broissia, Robert Calmejane, Auguste Cazalet, Xavier Darcos, Désiré Debavelaere, Luc Dejoie, Jacques Delong, Robert Del Picchia, Charles Descours, Yann Gaillard, Patrice Gélard, Alain Gérard, Charles Ginésy, Daniel Goulet, Alain Gournac, Georges Gruillot, Hubert Haenel, Jean-Paul Hugot, Roger Husson, André Jourdain, Christian de La Malène, Lucien Lanier, Robert Laufoaulu, Jacques Legendre, Guy Lemaire, Bernard Murat, Paul Natali, Mme Nelly Olin, MM. Joseph Ostermann, Jacques Oudin, Jacques Peyrat, Jean-Jacques Robert, Jean-Pierre Schosteck, Martial Taugourdeau et René Trégouët, sénateurs.

² Rapport « La nouvelle donne du commerce électronique : réalisation 1998 et perspective ».

La redéfinition de la preuve littérale indépendamment du support utilisé

Le projet de loi définit la preuve littérale afin de la rendre indépendante de son support (nouvel article 1316 du code civil).

Désormais, la preuve littérale ne s'identifiera plus au papier. Elle ne dépendra pas non plus des modalités de sa transmission, ce qui signifie que l'écrit restera un écrit même s'il est transféré ou stocké sous forme électronique, à condition qu'il puisse être à nouveau intelligible. Cette définition est suffisamment large pour être **technologiquement neutre**.

La valeur juridique du document électronique est équivalente à celle de l'acte sous seing privé

L'exposé des motifs du projet de loi présente, sous un même « chapeau », consacré à la reconnaissance explicite de la valeur juridique du document électronique, trois articles dont les finalités sont sensiblement différentes.

La recevabilité en mode de preuve du document électronique

L'article 1^{er} du projet de loi (article 1316-1 du code civil) reconnaît l'admissibilité comme mode de preuve de l'écrit électronique, au même titre que l'écrit sur support papier, à condition que les moyens techniques utilisés donnent des assurances, d'une part sur la bonne conservation du message, et d'autre part sur l'identité de celui dont émane l'écrit et auquel on entendrait l'opposer.

La force probante du document électronique est équivalente à celle de l'acte sous seing privé

L'article 2 du projet de loi (article 1322-1 du code civil) reconnaît à l'écrit électronique qui constate des droits et obligations et qui porte une signature, une force probante équivalente à celle d'un acte sous seing privé sur support papier.

Le choix n'a donc pas été fait de hiérarchiser la force probante des documents selon le support utilisé (voir *infra*), c'est-à-dire de conférer à l'écrit électronique un statut « inférieur » à celui de l'écrit sur support papier.

La suppression des mentions manuscrites

L'article 4 du projet de loi propose de lever l'obstacle à l'utilisation du document électronique que constitue la formalité de la mention manuscrite de la somme en toutes lettres et en chiffres exigée pour les actes unilatéraux (article 1326 du code civil).

Constatant que le code civil ne contient actuellement aucun article réglant les conflits entre preuves littérales, le projet de loi propose que le juge qui lui sont soumis. Le juge du fond déterminera souverainement au cas par cas, en tenant compte de toutes les circonstances de l'espèce, quelle est la

Les conventions sur la preuve

L'article 1341 du code civil sur la préconstitution de preuve par écrit des conventions sur la preuve. Le projet de loi propose de lever toute incertitude sur la portée exacte de cette jurisprudence en consacrant cette

La définition générale de la signature et la reconnaissance de la signature électronique

Le projet de loi comporte une définition de la signature qui fait ressortir clairement ses deux fonctions, qu'elle soit manuscrite ou non signature renseigne sur l'identité de l'auteur de l'acte et manifeste l'adhésion du signataire au contenu de l'acte (article 1322-1 du code civil).

Le projet de loi consacre la validité des procédés dits de signature électronique et précise à quelles conditions une signature peut être admise sous

Le projet de loi s'inscrit pleinement dans le cadre de la directive communautaire puisqu'il instaure une présomption de fiabilité au bénéfice des par décret en Conseil d'Etat.

LA POSITION DE VOTRE COMMISSION DES LOIS : ÉTENDRE LE CHAMP D'APPLICATION DU PROJET DE LOI AUX ACTES AUTHENTIQUES

BIEN MESURER LA PORTÉE DE LA STRICTE ÉGALITÉ ENTRE SUPPORT PAPIER ET SUPPORT ÉLECTRONIQUE

Votre commission des Lois souligne la portée fondamentale de l'égalité instituée par le projet de loi entre la force probante de l'écrit sur support papier et celle de l'écrit électronique signé.

Comme en matière de commerce électronique, votre rapporteur souhaite que le débat porte sur les questions juridiques, même si les aspects techniques ne doivent pas être ignorés ; ils relèvent du pouvoir réglementaire, exercé par le Gouvernement sous le contrôle du Parlement.

A cet égard, l'argument selon lequel la signature électronique serait beaucoup plus sûre que la signature manuscrite est sans doute recevable sur le plan technique.

Lors de l'audition des représentants de la société IBM, convaincante sur le plan technique, votre commission a pu observer que le commerce traditionnel donnerait lieu aujourd'hui à environ 1 % de litiges, tandis que le commerce électronique susciterait 15 à 37 % de contentieux, portant essentiellement sur les paiements.

Sur le plan juridique, il ne devrait pas être exclu d'accorder à la signature manuscrite une valeur supérieure à la signature électronique. Le législateur ne doit pas se voir imposer certaines solutions juridiques au motif qu'elles correspondent à l'état de la technique.

Il aurait pu par exemple considérer que l'écrit électronique, qui peut être modifié à tout moment, est **un écrit sur support réversible**, tandis que l'écrit papier est **un écrit sur support altérable**, et refuser en conséquence l'égalité entre support papier et support électronique.

Votre commission des Lois n'a pas fait ce choix, dans la mesure où il aurait été **contraire au droit communautaire**.

DISTINGUER ÉCRIT « AD VALIDITATEM » ET ÉCRIT « AD PROBATIONEM »

La distinction entre valeur *ad validitatem* et valeur *ad probationem* d'un acte juridique

L'écrit requis « ad solemnitatem » ou « ad validitatem »

La solennité de certains actes exige que la volonté s'exprime par écrit et, par conséquent, qu'ils soient établis sous une forme préconstituée. Leur rédaction est alors une condition de **l'existence** même du droit.

En exigeant un écrit, le législateur a parfois recherché **la protection des intérêts des contractants** et non la simple préconstitution de preuve. Dans ce cas, l'exigence d'un écrit est imposée par le législateur « **à peine de nullité** » ; on dit couramment que l'écrit est exigé *ad solemnitatem*¹ ou *ad validitatem*.

Le problème de la preuve est « absorbé » par celui de la validité, en ce sens qu'en l'absence d'un écrit dressé dans les formes légales, l'acte ne peut pas être prouvé parce que, juridiquement, il n'existe pas.

L'écrit requis « ad probationem »

Le législateur a parfois imposé la rédaction d'un écrit, sans pour autant prévoir une sanction. Il n'est alors requis que pour faire preuve. Cependant, la loi n'est pas toujours explicite en la matière et les dispositions sont de plus en plus nombreuses qui prévoient un écrit, au moins sous seing privé, pour certains contrats, sans en préciser la portée. Le juge doit alors déterminer si l'écrit est exigé *ad validitatem* ou *ad probationem*.

Votre commission des Lois souhaite réserver la reconnaissance de l'écrit électronique aux écrits *ad probationem*

Dans un précédent rapport, consacré à une proposition de résolution de la Délégation du Sénat pour l'Union européenne, sur la proposition de directive communautaire relative à certains aspects juridiques du commerce électronique, votre rapporteur soulevait déjà la question de la compatibilité avec la directive proposée du droit national relatif à l'**existence** et à la **valeur probante** des écrits sous forme électronique.

¹ Dans le langage courant, l'acte est dit solennel lorsque la forme requise par la loi est un acte authentique. Il en va ainsi pour la donation entre vifs, la constitution d'hypothèque, le contrat de mariage notamment.

Mais en droit positif, la distinction entre écrits *ad probationem* et écrits *ad validitatem* ne recoupe pas la distinction entre actes sous seing privé et actes authentiques. En effet, de nombreux actes authentiques relèvent de l'écrit *ad probationem*, et à l'inverse certains actes sous seing privé sont requis *ad validitatem*.

Votre commission des Lois, constatant que la directive proposée ne posait aucune condition pour la reconnaissance de l'efficacité juridique du contrat passé par voie électronique, avait souligné **la nécessité de maintenir l'exigence d'écrits *ad validitatem* dans de nombreux domaines**, regrettant l'insuffisance des exceptions prévues par la directive proposée.

Elle ajoutait que de nombreux contrats, en raison de leur gravité, ne devraient pas être admis par voie électronique, soulignant que le droit français comportait de nombreuses prescriptions quant à la formalité des contrats, en exigeant un écrit *ad validitatem*.

Elle a donc souhaité que l'adaptation de ces prescriptions aux technologies de l'information ne résulte pas d'une disposition générale dont les implications n'auraient pas été mesurées, mais qu'elle donne lieu à un débat et un examen approfondis.

En conséquence, elle demandait au Gouvernement de s'assurer que la levée des obstacles juridiques à la conclusion des contrats électroniques laisse subsister des moyens de preuve suffisants.

Pour ces raisons, votre commission des Lois vous proposera **d'interroger le Gouvernement sur la suppression des exigences formelles imposées à l'acte sous seing privé unilatéral** (article 4 du projet de loi).

INCLURE LES ACTES AUTHENTIQUES

Votre commission des Lois constate que le projet de loi intéresse les seuls actes sous seing privé sur support électronique. Elle vous propose **d'inclure les actes authentiques dans le champ d'application du projet de loi**.

Même si les actes authentiques électroniques ne seront pas immédiatement mis en œuvre, il importe de les rendre possibles, en renvoyant au pouvoir réglementaire la question des modalités de mise en œuvre.

Cette solution évite que le législateur n'ait à modifier à nouveau le code civil d'ici quelques années pour admettre l'acte authentique sur support électronique. De plus, le législateur pourra intervenir ultérieurement pour modifier les règles particulières spécifiques à chacune des catégories d'actes authentiques.

Votre commission des Lois vous proposera ainsi que les actes authentiques puissent être établis et conservés sur support électronique, sous réserve qu'ils répondent à des conditions fixées par décret en Conseil d'Etat (article additionnel après l'article 1^{er}).

En complément, elle vous proposera de **définir la signature de l'officier public** (article 3 du projet de loi).

De plus, elle vous proposera de faire figurer la qualification de la force probante de l'écrit sur support électronique dans les dispositions générales relatives à la preuve littérale, au lieu d'en limiter l'application aux actes sous seing privé.

Enfin, elle vous proposera de soumettre la forme probante de l'écrit sur support électronique au respect des conditions de forme touchant à la validité de l'acte.

NE PAS SOUS-ESTIMER LES ASPECTS RÉGLEMENTAIRES

La directive communautaire sur les signatures électroniques détaille les aspects techniques qui, en France, seront transposés par voie réglementaire. Les enjeux en sont importants, puisqu'il s'agit d'instaurer un marché intérieur des services de certification. Ce nouveau métier, qui reste à inventer, pourrait générer d'importants chiffres d'affaires à terme.

*

* *

Sous réserve de ces observations et des modifications qu'elle vous soumet, votre commission des Lois vous propose d'adopter le projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique.

EXAMEN DES ARTICLES

Article 1^{er}

(art. 1315-1, 1316, 1316-1 et 1316-2 du code civil)

Subdivisions du code civil relatives à la preuve

Cet article réaménage les subdivisions du code civil relatives à la preuve puis introduit des dispositions générales sur l'écrit électronique et la preuve littérale.

I. Énumération des règles de preuve

Le paragraphe I de cet article renumérote l'article 1316 du code civil, qui devient l'article 1315-1. Il s'agit d'un simple aménagement formel.

L'article 1316 actuellement en vigueur présente le plan du chapitre VI du titre III du livre troisième du code civil, consacré à la preuve des obligations et à celle des paiements. Il indique que les règles qui concernent la preuve littérale, la preuve testimoniale, les présomptions, l'aveu de la partie et le serment sont expliquées dans les sections suivantes du code.

En droit civil, le juge ne doit former sa conviction que d'après les moyens de preuve admis par la loi. La preuve n'est réputée légalement faite que si elle est administrée suivant les formes prescrites, c'est-à-dire par écrit, par témoin, par présomption, par aveu ou par serment.

Le choix d'inscrire l'écrit électronique dans la subdivision du code civil consacrée à la preuve est fondamental. Il traduit l'orientation du projet de loi de ne pas modifier les exigences d'écrit sur support papier pour la validité juridique des actes (écrits *ad validitatem*) et de n'affecter que leur force probante (écrits *ad probationem*).

II. Renumérotation des paragraphes de la section du code civil consacrée à la preuve littérale

Le paragraphe II du présent article est purement formel, il renumérote les cinq paragraphes de la section première, consacrée à la preuve littérale, du chapitre VI du titre troisième du livre troisième du code civil.

Cette nouvelle structure permet d'introduire un « chapeau » dans le droit de la preuve littérale.

Les paragraphes actuels de cette section sont consacrés respectivement au titre authentique, à l'acte sous seing privé, aux tailles, aux copies des titres et aux actes récongnitifs et confirmatifs.

III. Dispositions générales relatives à la preuve par écrit

Le paragraphe III du présent article tend à insérer un nouveau paragraphe dans la section relative à la preuve littérale, afin de prévoir des **dispositions générales**, qui vaudront aussi bien pour l'acte authentique et l'acte sous seing privé que pour les autres catégories de preuve par écrit.

Ce nouveau paragraphe premier contiendrait trois articles :

- la définition de la preuve littérale indépendamment du support utilisé (nouvel article 1316 du code civil) ;

- l'admissibilité en mode de preuve de l'écrit sur support électronique (article 1316-1) ;

- la reconnaissance des conventions sur la preuve et le règlement des conflits de preuve (article 1316-2).

Paragraphe 1^{er} de la section première du chapitre VI du titre troisième du Livre troisième du code civil Dispositions générales relatives à la preuve par écrit

Cet article tend à créer une nouvelle subdivision dans le code civil, réunissant les dispositions générales relatives à la preuve par écrit. Ce nouveau paragraphe comprendra trois articles (articles 1316 à 1316-2 du code civil).

Article 1316 du code civil

Définition de la preuve littérale indépendamment de son support

Ce nouvel article 1316, placé en tête de la section consacrée à la preuve littérale, propose **une définition de la preuve par écrit indépendamment du support utilisé.**

Votre commission des Lois vous propose **un amendement** rédactionnel permettant de lever une confusion possible, la « *preuve par écrit* » étant l'exact synonyme de la « *preuve littérale* ».

Selon cet article, 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.

Il vise à revenir sur l'assimilation historique de la preuve littérale au support papier. En effet, comme le souligne l'exposé des motifs du projet de loi, les dispositions du code civil sur la preuve ont été rédigées à une époque où le papier était le seul support utilisé pour constater l'existence et le contenu des contrats et en faire la preuve.

Dans la mesure où elle figure dans la subdivision du code civil consacrée à la preuve, cette définition ne concerne que l'écrit exigé *ad probationem* et reste sans incidence sur l'écrit exigé *ad validitatem*.

Article 1316-1 du code civil

Admissibilité en mode de preuve de l'écrit électronique

Cet article vise à la **reconnaissance explicite de la valeur juridique du document électronique**.

Il reconnaît l'admissibilité en mode de preuve de l'écrit électronique, au même titre que l'écrit sur support papier, sous deux conditions :

- que puisse être dûment **identifiée** la personne dont il émane ;
- qu'il soit établi et conservé dans des conditions de nature à en garantir l'**intégrité**.

1. Une reconnaissance légale du document électronique qui s'inspire de la jurisprudence

La jurisprudence de la chambre commerciale de la Cour de cassation du 2 décembre 1997 pose déjà les deux conditions : authentification des parties, intégrité du message. L'écrit peut être établi et conservé sur tout support, y compris par télécopie, dès lors que son **intégrité** et l'**imputabilité** de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées. Cette jurisprudence, relative à une télécopie portant sur une cession de créance entre commerçants dont le contenu n'est pas contesté, n'a qu'une portée limitée.

2. Rappel de la jurisprudence sur les photocopies et télécopies

La jurisprudence a pris en compte dans une certaine mesure l'apparition de formes modernes de reproduction et de transmission des documents.

a) Le cas des photocopies

En principe, **les reproductions photographiques d'actes sous seing privé ne peuvent servir ni de preuve ni de commencement de preuve par écrit**¹. Il en va de même lorsque la photocopie a fait l'objet d'une certification, en application du principe posé par l'article 1334 du code civil¹ selon lequel seul l'original fait foi. Il est donc du pouvoir souverain du juge du fond, à qui il appartient d'apprécier la force probante des documents qui lui sont soumis, d'écarter une photocopie.

Il existe des **exceptions** à ce principe : un écrit non représenté peut être invoqué conformément à l'article 1347 du code civil (c'est-à-dire comme commencement de preuve par écrit) dès lors que son existence et son contenu sont établis d'une manière certaine, soit à la suite d'un aveu de l'adversaire, soit comme conséquence du serment décisoire déferé au plaideur à qui ce commencement de preuve est opposé.

Ainsi, **une photocopie dont la conformité avec l'original n'est pas contestée peut servir de commencement de preuve par écrit**, dans la mesure où cet original le constituerait également.

b) En matière de télécopie et de télex, la jurisprudence a pu sembler incertaine.

La valeur probante de la télécopie varie suivant les domaines dans lesquels elle est utilisée et les stipulations contractuelles des parties :

- en matière commerciale, la règle de la liberté de la preuve des actes de commerce à l'égard des commerçants (article 109 du code de commerce) permet aux parties de faire la preuve du contrat par tous moyens ;

- en matière civile, les actes juridiques dont l'objet est inférieur à 5.000 francs échappent à l'exigence de la préconstitution d'un écrit à titre de preuve.

Dans ces deux hypothèses, la télécopie peut être utilisée comme mode de preuve, mais sa valeur probante sera appréciée par le juge en fonction des garanties de sécurité et de **fiabilité** qu'elle présente.

- toujours en matière civile, pour les actes juridiques dont l'objet excède la valeur de 5.000 francs, l'obligation de préconstituer la preuve par écrit et l'interdiction de prouver par témoignage ou présomptions contre et outre le contenu des écrits **s'opposent à ce que la télécopie puisse être utilisée comme mode de preuve.**

¹ Cour de cassation, chambre commerciale, 20 décembre 1976.

Dans ce cas, les **exceptions énoncées aux articles 1347 et 1348 du code civil** soumettent à l'appréciation des tribunaux la valeur accordée à un document transmis par télécopie.

Ainsi, lorsqu'elle émane de celui auquel on l'oppose, la télécopie pourrait être considérée comme valant commencement de preuve par écrit. Dans d'autres circonstances, une jurisprudence récente de la chambre civile de la cour d'appel de Limoges, en date du 18 mars 1999, indique qu'une télécopie, même si elle comporte une signature, ne peut, en l'absence de tout commencement de preuve par écrit émanant du débiteur prétendu de l'obligation, revêtir la moindre force probante.

De plus, il est loisible aux parties de reconnaître conventionnellement une force probante particulière aux télécopies échangées entre elles, dans la mesure où les prescriptions de l'article 1341 du code civil ne sont pas d'ordre public.

Saisi d'un litige ayant trait à un moyen de communication télématique, à défaut de stipulations contractuelles leur conférant une valeur probante déterminée, **le juge apprécie souverainement s'ils offrent une fiabilité suffisante pour établir la preuve de ce qui est allégué.**

A ce titre, la télécopie présente une différence fondamentale avec la photocopie, dans la mesure où elle est la photocopie d'un original que n'a jamais détenu celui qui la reçoit.

La télécopie est donc un élément de preuve supérieur à la photocopie ; pour le destinataire, la télécopie peut valoir commencement de preuve par écrit ; mais sa production de la part de l'émetteur ne devrait constituer qu'une présomption, et non un commencement de preuve par écrit, pour la simple raison que l'écrit émane de celui qui le produit.

Enfin, il semblerait que ces experts s'accordent à considérer que le télex constitue un élément de preuve plus fiable que la télécopie.

3. Le projet de loi satisfait la proposition de loi n° 244

La proposition de loi n° 244 tend à reconnaître la valeur probante de la télécopie. Votre rapporteur estime qu'une confusion doit être évitée, dans la mesure où l'exposé des motifs de la proposition de loi ne correspond pas tout à fait à la modification du code civil qu'elle propose.

En effet, l'exposé des motifs ne traite que des relations **en matière commerciale**. Or, dans ce domaine, la preuve est libre : les télécopies font foi entre les parties et le juge examine l'imputabilité du contenu de l'acte à son auteur et l'intégrité de ce contenu. Il est possible d'inscrire dans la loi une jurisprudence particulière afin de lui conférer valeur législative et solennité.

¹ L'article 1334 du code civil dispose : « Les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la présentation peut toujours être exigée ».

Cependant, cette jurisprudence étant bien établie, votre commission des Lois n'estime pas cette précision nécessaire.

De plus, si cette proposition de loi, contrairement à ce que son exposé des motifs laisse entendre, vise à modifier les règles de preuve **en matière civile**, votre rapporteur constate qu'elle est satisfaite par la rédaction :

- de l'article 1316 du code civil proposée par le projet de loi, qui définit la preuve littérale indépendamment de son support et surtout **indépendamment de ses modalités de transmission**,

- ainsi que par l'article 1316-2 permettant au juge de déterminer les écrits -transmis éventuellement par voie télématique ou électronique- les plus vraisemblables, *quel qu'en soit le support*.

4. L'intégrité, une notion peu juridique

Une difficulté résulte du mélange entre le vocabulaire technique et le vocabulaire juridique et du fait que le terme d'intégrité n'est pas défini dans le projet de loi. D'après le dictionnaire, est intègre l'objet qui n'a pas été modifié, intentionnellement ou non, par rapport à un état antérieur.

5. Identification ou imputabilité ?

Lors des auditions qu'il a menées, votre rapporteur a été saisi de propositions tendant à affirmer que seule peut être dûment identifiée la personne **à laquelle est imputable** un document électronique, et non la personne **dont il émane** effectivement.

La notion d'**imputabilité** permettrait ainsi d'engager la responsabilité de la personne qui a « prêté » sa signature électronique à une autre personne et conteste ensuite le document ainsi signé.

Selon le projet de loi, la personne qui a divulgué sa clé privée et le code secret permettant de l'utiliser à une tierce personne (utilisant le même ordinateur), pourrait faire valoir que le document litigieux n'émane pas d'elle et qu'elle n'a pas consenti aux obligations qu'il reconnaît. Il en va de même pour la personne à laquelle ont été subtilisés ces éléments. La notion d'imputabilité rendrait plus difficile cette contestation.

Votre rapporteur souligne l'intérêt de reconnaître que l'écrit sur support électronique ne peut être admis en mode de preuve que dès lors qu'est identifiée la personne dont il émane, c'est-à-dire la personne qui a matériellement émis le message électronique.

En effet, le droit français reconnaît l'imputabilité indirecte, c'est-à-dire qu'une faute peut émaner d'une personne mais être imputable à une autre, par exemple dans le cas de la responsabilité du fait d'autrui.

Votre rapporteur rappelle que la notion d'imputabilité emporte des effets juridiques alors que le projet de loi emploie délibérément un langage courant, neutre, permettant au juge, en cas de conflit, de vérifier de quelle personne émane effectivement le document litigieux. En conséquence, **il lui paraît hasardeux de substituer la notion d'imputabilité à celle de l'identification de la personne dont émane le document.**

6. La conservation des documents électroniques

La durée de conservation des actes est de **dix ans en matière commerciale et de trente ans en matière civile.**

La loi n'apporte aucune précision quant aux formes de l'archivage. Elle prévoit seulement la possibilité de présenter, à titre de commencement de preuve par écrit, une copie qui soit une reproduction fidèle et durable de l'original (second alinéa de l'article 1348 du code civil).

L'admission de l'écrit électronique en moyen de preuve suppose qu'il soit établi **et conservé** dans des conditions de nature à en garantir l'intégrité. Les conditions de fiabilité concernant les moyens de conservation des documents électroniques signés seront fixées par voie réglementaire.

La **proposition de loi n° 246** propose la conservation fiable du document sous le contrôle de son signataire. Votre rapporteur indique que ce contrôle pourrait être indirect, au moyen des « tiers de confiance » prévus par la directive européenne sur les signatures électroniques. En effet, certains prestataires conserveront non seulement les clés relatives à la signature des utilisateurs, mais aussi les documents échangés¹.

La **conservation des moyens de preuve**² sur support électronique pose le problème de l'inégalité entre les parties ; elle risque fort d'être **unilatérale**, seuls les professionnels disposant des moyens techniques d'archiver les documents électroniques sur une longue durée (celle de la prescription).

En effet, en raison de l'évolution très rapide des techniques, il est difficile de garantir que l'intéressé disposera bien au moment voulu, des interfaces logicielles et matérielles requises pour accéder à la lecture du document sur support électronique établi dix ans plus tôt.

Dès lors, il a pu paraître souhaitable à certains commentateurs de laisser libre la preuve contraire permettant de contester en cas de besoin l'écrit électronique, ou d'autoriser la preuve contraire sur le fondement de présomptions graves, précises et concordantes.

¹ Votre rapporteur fait ici référence au service développé par La Poste, dit « Pasrel », lancé en novembre 1999.

² L'AFNOR a publié une norme sur l'archivage des documents électroniques (norme AFNOR NFZ 42013). Elle propose la recopie périodique des documents.

Article 1316-2 du code civil
Règlement des conflits de preuve littérale
Conventions sur la preuve

Cet article a un double objet :

- il confie au juge le soin de régler les conflits de preuve littérale ;
- il reconnaît dans la loi la validité des conventions sur la preuve.

1. Le juge règle les conflits de preuve littérale

Actuellement, le code civil ne contient aucune disposition réglant les conflits entre preuves littérales. Le présent article propose que le juge règle ces conflits en se fondant sur la vraisemblance des éléments qui lui sont soumis.

La **proposition de loi n° 246** tend à permettre aux juges de procéder à toutes les investigations techniques qu'ils estiment nécessaires pour établir l'authentification de la signature électronique.

Votre rapporteur souligne que le projet de loi (article 1316-2 du code civil) confie au juge le soin d'examiner les questions relatives à l'identification de l'auteur du document (authentification des parties). Quant à la fiabilité de la signature électronique, elle sera présumée dès lors que la signature remplira les conditions fixées par décret en Conseil d'Etat. Le rôle du juge est ainsi reconnu par l'article 1322-2 du code civil proposé par le projet de loi, puisque le régime de présomption légale de fiabilité ne s'applique que jusqu'à preuve du contraire. En conséquence, votre commission des Lois estime que la proposition de loi n° 246 est satisfaite sur ce point.

2. « Le titre le plus vraisemblable »

La notion de « vraisemblance » peut paraître *a priori* subjective. Elle est déjà utilisée par le juge, puisque l'article 1347 du code civil définit le commencement de preuve par écrit comme l'écrit qui rend **vraisemblable** le fait allégué. L'acte doit permettre une approche de la vérité, faire présumer celle-ci sans la prouver entièrement. La qualification de la vraisemblance relève du pouvoir exclusif des juges du fond et échappe au contrôle de la Cour de cassation.

3. Validité des conventions sur la preuve

Le présent article tend également à inscrire dans la loi les solutions apportées par la jurisprudence, reconnaissant la possibilité de passer des conventions sur la preuve dérogeant aux règles supplétives contenues dans le code civil.

En effet, **l'article 1341 du code civil relatif à l'exigence de l'écrit n'est pas d'ordre public**. Il est possible d'y déroger par convention, en fixant d'autres moyens de preuve, tels que le recours au document électronique.

Actuellement, les entreprises recourent à des conventions d'échange élaborées dans le cadre des EDI¹. Une convention d'échange a pour objet d'indiquer quels sont les messages qui seront transférés par voie d'EDI et de prévoir comment seront résolus les éventuels litiges concernant le contenu des messages dématérialisés qui ont été échangés.

La jurisprudence admet déjà la **validité des conventions** portant sur la signature informatique **en matière de paiement par cartes bancaires**². Selon le rapport annuel de la Cour de cassation pour 1989, *ce procédé présente les mêmes garanties que la signature manuscrite, laquelle peut être imitée tandis que le code secret n'est connu que du seul titulaire de la carte* ».

La loi et la jurisprudence prescrivent certaines limites pour **éviter les déséquilibres entre les parties** : la convention ne doit pas avoir pour objet ou pour effet d'avantager celui qui en est l'initiateur ou le rédacteur. La possibilité de rapporter la preuve contraire doit être systématiquement garantie. Dans les relations avec les consommateurs, la loi n° 95-96 du 1^{er} janvier 1995 sur les **clauses abusives** est pleinement applicable.

Les conditions minimales de validité des conventions sur la preuve seraient ainsi l'absence de déséquilibre entre les parties et la possibilité de rapporter la preuve contraire.

Dans le même ordre d'idées, le Conseil d'État, craignant que certaines conventions ne contiennent des clauses abusives, en recommande un usage « subsidiaire et encadré ».

Article additionnel après l'article 1^{er}
(art. 1317-1 du code civil)

Actes authentiques

Le projet de loi ne s'applique pas aux actes authentiques. En effet, la définition de la force probante du document électronique n'est envisagée que pour les actes sous seing privé (voir l'article 2 du projet de loi) et la définition de la signature en général et de la signature électronique ne s'applique qu'aux actes sous seing privé (article 3 du projet de loi).

¹ L'EDI désigne l'échange par voie électronique de données structurées, organisées en messages normalisés.

² En vertu de l'arrêt CREDICAS de la Cour de cassation en date du 8 novembre 1989, dans le cadre d'une convention de preuve, la validité de la signature par code secret des paiements par carte bancaire est admise.

Votre commission des Lois ne souhaite pas traiter différemment les actes sous seing privé et les « actes sous seing public » que sont les actes authentiques.

Elle vous soumet donc **un amendement** tendant à insérer **un article additionnel** après l'article premier.

Elle vous propose de poser une règle générale **admettant l'acte authentique électronique** dans l'article 1317 du code civil. Ainsi, l'acte authentique pourra être dressé sur support électronique s'il est établi et conservé dans des conditions de sécurité fixées par décret en Conseil d'Etat.

1. Le régime juridique des actes authentiques.

En vertu de l'article 1317 du code civil, l'acte authentique est celui qui a été **reçu par officiers publics** ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les **solennités requises**. L'acte qui n'est pas authentique vaut comme écriture privée, s'il a été signé des parties. L'acte authentique fait pleine foi de la convention qu'il renferme entre les parties contractantes.

L'acte authentique est reçu par un officier public répondant à des conditions de compétence (compétences d'attribution et territoriale) et de capacité (en fonction par exemple de l'intérêt que l'officier public peut avoir à l'acte).

La « **réception** » par un officier public signifie qu'il recueille le consentement des parties. La condition de réception implique à la fois la **présence** de l'officier public lors de la manifestation de volonté enregistrée ou des faits constatés, et la **signature** de l'acte par l'officier public.

Les solennités requises désignent en particulier les garanties de conservation présentées par l'acte authentique : le fait que l'original est **établi en un seul exemplaire**, conservé dans la **minute** des notaires, si bien que l'original n'est pas dans les mains d'une des parties.

L'authenticité a deux conséquences : **force probante de très haut niveau et force exécutoire**.

2. La vérification du consentement des parties

La solution proposée par votre commission des Lois ne modifie aucunement le formalisme¹ de l'acte authentique.

¹ *Le support utilisé doit être bien distingué de la forme de l'acte. L'acte authentique continuera à être établi avec les formalités requises, mais il pourra être admis en mode de preuve s'il est établi sur support électronique, et, sous condition de fiabilité liée à la signature électronique utilisée, il aura la même force probante que l'acte authentique sur support papier.*

Votre rapporteur souhaite bien distinguer le support électronique du transport électronique : le transport suppose une distance entre les deux parties, qui pose un problème d'authentification. Lorsque les contractants seront à distance, et qu'un officier public vérifiera le **consentement** d'une des parties, il est essentiel que l'officier public engage sa responsabilité vis-à-vis de la personne : il doit s'assurer que la personne a bien compris la portée de son engagement.

Pour les actes qui engagent dans une forte proportion le patrimoine ou l'avenir de l'entreprise ou de son dirigeant (contrats complexes, de longue durée, actes de cautionnement...), la nécessité de négocier les termes du contrat fait que **la réunion physique des personnes continuera à rester la règle.**

Même si la validation finale du contrat s'effectue par voie électronique, on ne pourra pas en déduire pour autant que ces parties n'ont pas **une connaissance exacte de l'objet et de la portée de leur engagement.**

L'acte authentique électronique devra être établi en présence de l'officier public et de la personne concernée ; ensuite, il peut être envisagé :

- de le transmettre à l'autre partie, en présence d'un autre ou du même officier public ;
- de la conserver sous forme électronique.

La relation humaine *intuitu personae* est indispensable pour s'assurer de la capacité et du consentement de la personne ; elle n'est pas remise en cause par l'admissibilité en mode de preuve de l'acte authentique électronique et la reconnaissance de sa force probante.

3. La reconnaissance de la force probante de l'acte authentique électronique vaut pour l'avenir

L'amendement proposé par votre commission des Lois rend possible la reconnaissance **ultérieure** des actes authentiques électroniques. Cette solution permet d'éviter une nouvelle modification du code civil d'ici quelques années, lorsque les officiers publics et ministériels disposeront des moyens logiciels et matériels leur permettant de transmettre les actes authentiques par voie électronique.

Il s'agit de ne pas fermer la porte à ce qui deviendra un jour l'authenticité électronique. Le renvoi au décret en Conseil d'Etat permettra de mettre en œuvre l'acte authentique électronique dès que les conditions matérielles le rendront possible.

Une modification ultérieure de la loi du 25 Ventôse an XI contenant organisation du notariat est envisageable, s'il apparaît que la reconnaissance de l'acte authentique électronique requiert une modification du régime des actes notariés. En tout état de cause, elle sera soumise à l'examen du Parlement.

Article 2

(art. 1322-1 du code civil)

Force probante équivalente à celle de l'acte sous seing privé

Cet article reconnaît à l'écrit électronique, qui constate des droits et obligations et qui comporte une signature, **une force probante équivalente à celle d'un acte sous seing privé sur support papier.**

Formellement, il crée un article 1322-1 dans le deuxième paragraphe de la section première du code civil sur la preuve littérale, relatif à l'acte sous seing privé. Le champ d'application de cet article est donc limité aux actes sous seing privé.

Il doit être lu par référence à l'article 1322 du code civil, selon lequel *« l'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a, entre ceux qui l'ont souscrit et entre leurs héritiers et ayants cause, la même foi que l'acte authentique ».*

1. Régime juridique de l'acte sous seing privé

En dehors des exceptions prévues par la loi, l'acte sous seing privé n'est soumis à aucune autre **condition de forme que la signature de ceux qui s'obligent**. En d'autres termes, un acte vaut comme acte sous seing privé dès lors qu'il a été signé par la partie à qui on l'oppose et qu'il est invoqué par la partie à qui il a été remis.

Un acte sous seing privé n'a de force probante qu'autant que la signature en est expressément ou tacitement reconnue ou a été au préalable vérifiée en justice. Lorsque la signature est déniée ou méconnue, il appartient à celui qui se prévaut de l'acte de prouver sa sincérité.

Les actes sous seing privé ne font foi que jusqu'à preuve contraire de la sincérité des faits juridiques qu'ils constatent et des énonciations qu'ils contiennent.

2. La force probante d'un écrit électronique

Le projet de loi propose la faculté d'assimiler un document électronique à un écrit sous seing privé à deux conditions : intégrité des données (y compris lors de leur conservation future) et imputabilité du message au signataire ainsi identifié. L'article 1322-1 confère à l'écrit électronique la même force probante que celle de l'acte sous seing privé sur support papier, reconnu par celui auquel on l'oppose ou légalement tenu pour reconnu.

3. L'insertion dans le code civil

L'article 1322-1 ne répète pas les termes de l'article 1316-1, ces deux articles ayant des champs d'application bien distincts :

- l'article 1316-1 vise l'**écrit** quel qu'il soit ; il n'est pas obligatoirement signé ; il peut s'agir en outre aussi bien d'un acte sous seing privé que d'un acte authentique ;

- l'article 1322-1 vise les **actes juridiques** créateurs de droits et d'obligations. Il s'applique clairement aux **contrats**. Il s'agit d'une application particulière (inscrite dans la subdivision consacrée aux actes sous seing privé) de la règle (inscrite dans les dispositions générales) posée par l'article 1316-1. L'écrit visé à l'article 1322-1 doit être **signé** pour être un acte créateur de droits et d'obligations. La signature est en effet nécessaire à la perfection d'un acte sous seing privé.

Votre commission juge contradictoire la rédaction de l'article 1322-1 proposée par le projet de loi.

En effet, cet article renvoie à l'article 1322, qui ne vise que l'acte sous seing privé **non contesté par celui auquel on l'oppose**. Or, on ne se préoccupe de la force probante d'un acte sous seing privé qu'en cas de contestation. Il ne paraît pas logique de conférer à l'acte électronique signé constatant des droits et obligations la même force probante¹ que celle de l'acte sous seing privé **non contesté**.

Votre commission des lois vous propose **un amendement** tendant à indiquer que la même force probante est attachée à l'écrit sur support papier ou sur support électronique, dès lors qu'il réunit toutes les conditions de forme nécessaires à sa validité.

4. La preuve contraire : comment prouver contre et outre l'écrit électronique ?

Les solutions hiérarchisant les modes de preuve en fonction du support n'ont pas été retenues par le projet de loi². Celui-ci retient au contraire une équivalence totale de la force probante de l'écrit sous forme électronique avec celle de l'écrit traditionnel.

Lorsqu'il ne sera pas signé, l'écrit électronique aura la force probante très limitée accordée aux écrits sur papier non signés (simple indice laissé à la

¹ C'est-à-dire la même force probante que l'acte authentique.

² Le Québec a modifié son code civil en 1993. Tout en reconnaissant la valeur probante des « inscriptions informatisées », le législateur a limité celle-ci en prévoyant que « le document reproduisant les données d'un acte juridique inscrites sur support informatique **peut être contredit par tous moyens** ».

Le GIP « Droit et Justice » proposait que l'écrit sous forme électronique puisse être combattu « sur le fondement de **présomptions graves, précises et concordantes** ».

libre appréciation du juge).

Lorsqu'il sera signé et aura été préétabli spécialement pour constater un acte générateur de droits et d'obligations, l'acte sur support électronique, ainsi devenu acte instrumentaire, aura exactement la même force probante que l'acte sous seing privé.

Conformément aux dispositions du projet de loi, combinées avec celles de l'article 1341 du code civil, **l'acte électronique signé ne pourra être combattu par des témoignages ou des présomptions, mêmes graves, précises et concordantes**, mais seulement par un autre acte, authentique ou sous seing privé, ou dans les conditions énoncées aux articles 1347 et 1348 du code civil.

Votre commission des Lois vous propose d'adopter l'article 2 **ainsi modifié**.

Article 3

(art. 1322-2 du code civil)

Définition de la signature et de la signature électronique

Cet article propose une définition générale de la signature puis inscrit la signature électronique dans le code civil.

Il insère un nouvel article 1322-2 après article 1322-1 du code civil précédemment créé, c'est-à-dire dans la subdivision consacrée aux actes sous seing privé.

La signature étant une condition d'existence de l'acte instrumentaire, la reconnaissance de l'existence d'un équivalent électronique à la preuve littérale traditionnelle serait privée de toute portée pratique si elle ne s'accompagnait pas d'une reconnaissance d'un équivalent électronique à la signature manuscrite.

1. La définition générale de la signature¹ est fonctionnelle

Aucun texte ne définit actuellement ce qu'il faut entendre par signature. Aux termes du premier alinéa de l'article 1322-2, « *la signature nécessaire à la perfection d'un acte sous seing privé **identifie** celui qui l'appose et manifeste son **consentement** aux obligations qui découlent de cet acte* ».

¹ En langage courant, la signature consiste dans l'apposition manuelle d'une marque distinctive destinée à s'approprier le contenu d'un acte.

Une **double fonction** sera assignée à la signature : identification de l'auteur de l'acte et manifestation de son consentement au contenu de l'acte. Cette définition couvre aussi bien la signature manuscrite que la signature électronique. Il existe une **équivalence fonctionnelle** entre signature manuscrite et signature électronique.

2. La question des actes authentiques

La preuve littérale est définie de manière générale, indépendamment de son support (article 1316 du code civil), alors que la signature définie à l'article 1322-2 serait celle « *nécessaire à la perfection d'un acte sous seing privé* ».

Rien ne semble justifier que la signature ne soit définie que dans la subdivision relative aux actes sous seing privé. Votre rapporteur souhaiterait inscrire la définition de la signature dans les dispositions générales relatives à la preuve littérale.

Cependant, cela souligne les difficultés juridiques ainsi soulevées. Le cas des actes sous seing privé est simple : la signature apposée manifeste le consentement du signataire aux obligations contenues dans l'acte. Mais, dans le cas d'un « acte sous seing public », la **signature de l'officier public** constitue une solennité et engage l'authentificateur qui doit avoir vérifié le consentement de la personne.

Dès lors, **reconnaître l'acte authentique électronique suppose de définir la signature de l'officier public authentificateur.**

Votre commission des Lois vous soumet **un amendement** tendant à donner une définition de la signature qui inclura les actes authentiques.

Formellement, cet amendement transfère les dispositions du présent article 3 du projet de loi dans les dispositions générales relatives à la preuve littérale (nouvel article 1316-4 du code civil).

Ainsi, la signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le 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.**

Cette réforme implique, pour chaque type d'acte authentique, de s'interroger sur sa recevabilité et sa force probante en cas d'utilisation du support électronique : les jugements ou les actes d'état civil doivent-ils être traités de la même façon que les actes notariés ou les actes des huissiers ?

Votre commission des Lois estime que les interventions législatives voire réglementaires nécessaires pour mettre en oeuvre l'acte authentique électronique, qui ne toucheront pas au code civil mais aux textes spécifiques à chaque catégorie d'acte authentique, indiqueront les conditions de la validité

des actes authentiques sur support électronique, en particulier les conditions de fiabilité de leur signature électronique.

3. La signature électronique est admise sous deux conditions

La définition de la signature électronique, conformément aux prescriptions de la directive communautaire sur les signatures électroniques, est « *technologiquement neutre* ».

La signature électronique consiste en l'usage d'un procédé **fiable** d'identification garantissant son **lien** avec l'acte auquel elle s'attache.

Le deuxième alinéa de l'article 1322-2 précise les conditions que doit remplir la signature électronique pour se voir reconnaître une valeur juridique, en des termes suffisamment généraux pour s'adapter aux évolutions techniques : fiabilité du processus employé ; lien indissociable entre la signature et le message.

L'article 2 de la proposition de loi n° 246 propose de même de reconnaître la force probante d'un document électronique à condition que soit possible l'identification par une signature électronique fiable et que soit assurée la conservation durable du message. Il est donc satisfait par le projet de loi.

Une application de la signature électronique mérite d'être soulignée : le décret n° 98-271 du 9 avril 1998 relatif à la carte de professionnel de santé porte reconnaissance par les administrations et les organismes de Sécurité Sociale de la signature électronique de la carte professionnelle de santé¹.

4. La signature électronique définie par le projet de loi est une signature élaborée

Le projet de loi reconnaît dans le code civil la signature « avancée », au sens de la directive communautaire, c'est-à-dire la signature qui est liée uniquement au signataire, permet de l'identifier, est créée par des moyens qu'il peut garder sous son contrôle exclusif et est liée aux données auxquelles elle se rapporte pour que toute modification ultérieure soit détectable.

Votre commission des lois estime que la traduction du terme « advanced signature » en « signature avancée » n'est pas satisfaisante. Il s'agit en fait d'**une signature élaborée, perfectionnée, indissolublement liée au texte auquel elle se rapporte**. Alors que la signature manuscrite est apposée au bas d'un texte, laissant la possibilité de blanc seing, la signature

¹ L'article R. 161-58 du code de la sécurité sociale dispose désormais : « Pour les applications télématiques et informatiques du secteur de la santé, la signature électronique produite par la carte de professionnel de santé est reconnue par les administrations de l'Etat et les organismes de Sécurité sociale comme garantissant l'identité et la qualité du titulaire de la carte ainsi que l'intégrité du document signé. Ainsi signés, les documents électroniques (...) sont opposables à leur signataire ».

électronique revient à signer chacun des mots du texte et leur enchaînement, pas une virgule du texte signé ne pouvant être modifiée sans que cela ne soit immédiatement visible pour le destinataire du message.

5. La fiabilité de la signature électronique relève d'un régime de présomption légale réfragable

La fiabilité du procédé de signature électronique 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.

Parmi ces exigences, conformément à la directive européenne sur les signatures électroniques, figure l'intervention de prestataires de services de certification.

Si le document est accompagné d'un **certificat** répondant à certaines exigences et délivré par une autorité de certification accréditée, la fiabilité de la signature, la conservation durable du document signé seraient présumées. La **charge de la preuve** serait alors inversée et incomberait à celui qui conteste le document.

Dans le cas contraire, celui qui se prévaut d'un document informatique signé mais non certifié devrait convaincre le juge que les conditions de fiabilité et de conservation durable sont dûment remplies.

6. Les aspects réglementaires de la signature électronique - la certification

La directive européenne du 13 décembre 1999 sur les signatures électroniques dispose dans son article 3 que les États membres ne soumettent la fourniture des services de certification à aucune autorisation préalable. Toutefois, les États peuvent instaurer ou maintenir des régimes volontaires d'accréditation. L'accréditation est reconnue comme un service public.

Le décret en Conseil d'État devrait organiser un régime d'accréditation volontaire des autorités de certification et préciser les exigences concernant les dispositifs de création de signature. Un organisme fixera les conditions de sécurité que doivent remplir les prestataires de service de certification.

L'article 3 de la proposition de loi n° 246 renvoie au décret d'application la définition des modalités de conservation durable du message électronique. Il est donc satisfait par l'article 3 du projet de loi.

7. La signature électronique est en fait un « sceau » électronique

Les prestataires de service de certification ont pour rôle d'authentifier le signataire, **en aucun cas de certifier le contenu du message.**

Le tiers certificateur ne garantit pas le consentement du signataire, il garantit la clé publique. En réalité, il garantit la correspondance entre la clé publique et l'identité déclarée du détenteur de la clé.

En revanche, **la certification de signature¹ par une autorité publique est bien plus puissante juridiquement** que la certification de clé publique par les tiers certificateurs.

Il s'agit d'un **sceau d'authenticité électronique** et non d'une « certification de signature » électronique.

La signature électronique est utilisée dans la perspective unique d'une transmission, la signature juridique dans la perspective de rendre parfait un acte sous seing privé.

Votre commission des Lois vous propose d'adopter l'article 3 **ainsi modifié.**

Article 4

(art. 1326 du code civil)

Mentions manuscrites

Cet article tend à remplacer la formalité exigée pour les **actes juridiques unilatéraux**, afin de lever les obstacles à l'utilisation du document électronique. Il modifie ainsi l'article 1326 du code civil², qui impose au débiteur d'écrire de sa main le montant de la somme d'argent qu'il doit au créancier. Le projet de loi prévoit que les mentions obligatoirement inscrites la partie qui s'engage pourront être écrites « **par elle-même** » et non plus « **de sa main** ».

¹ Par exemple la certification par le maire ou le commissaire de police à l'article L. 2122-30 du code général des collectivités territoriales : « Le maire, ou celui qui le remplace, est tenu de légaliser toute signature apposée en sa présence par l'un de ses administrés connu de lui, ou accompagné de deux témoins connus. Les signatures manuscrites données par des magistrats municipaux dans l'exercice de leurs fonctions administratives valent dans toute circonstance sans être légalisées par le représentant de l'Etat dans le département si elles sont accompagnées du sceau de la mairie. »

² L'article 1326 du code civil dispose : « L'acte juridique par lequel une seule partie s'engage envers une autre à lui payer une somme d'argent ou à lui livrer un bien fongible doit être constaté dans un titre qui comporte la signature de celui qui souscrit cet engagement ainsi que la mention, écrite de sa main, de la somme ou de la quantité en toutes lettres et en chiffres. En cas de différence, l'acte sous seing privé vaut pour la somme écrite en toute lettres. »

Il a été modifié par l'aloi n° 80-525 du 12 juillet 1980.

1. Régime juridique des mentions manuscrites

L'article 1326 du code civil prévoit des mentions manuscrites, requises pour faire la preuve d'actes sous seing privés unilatéraux. Ces mentions manuscrites sont communément appelées « bon pour » ou « lu et approuvé ».

Les actes authentiques ne sont pas visés par l'article 1326. Celui-ci n'est applicable qu'aux seuls actes contenant obligation, portant engagement de payer des sommes d'argent ou de fournir des choses fongibles. Il s'applique en particulier en matière de **cautionnement**, pour les contrats de prêts, et plus généralement pour toutes les **reconnaisances de dette** ¹

A défaut de la signature de celui qui s'engage, l'acte ne fait pas preuve de l'engagement. En l'absence de mention manuscrite de la somme écrite en chiffres, l'acte sous seing privé contenant l'engagement de caution est irrégulier et ne peut constituer qu'un commencement de preuve par écrit.

2. L'omission des formalités de l'article 1326 n'a pas toujours été considérée comme étant sans influence sur la *validité* de l'obligation elle-même.

Les exigences de l'article 1326 sont des règles de *preuve* qui ont pour finalité la protection du signataire.

Cependant, il a parfois été considéré qu'elles entraînaient des conséquences sur la *validité* même de l'acte. Dans le cas de cautionnement, il résulte de la combinaison des articles 1326 et 2015² du code civil que le cautionnement ne peut excéder la somme que la caution s'est engagée à payer telle qu'elle résulte de la mention écrite de sa main.

Il paraît souhaitable, en l'état actuel de la réflexion, de limiter les effets du projet de loi aux écrits requis *ad probationem*, et de ne procéder aux aménagements concernant les écrits *ad validitatem* qu'avec la plus grande prudence.

En conséquence, votre commission des Lois vous propose d'**interroger le Gouvernement sur la portée exacte de l'article 4**. Il s'agit de s'assurer du consentement des personnes reconnaissant une dette ou se portant caution, les mentions manuscrites étant censées attirer l'attention du débiteur sur la portée de son engagement. Les conditions de forme imposées à peine de nullité ne doivent pas être modifiées à l'occasion de l'examen du présent projet de loi.

¹ La reconnaissance de dette est soumise aux exigences de l'article 1341 du code civil (préconstitution de preuve par écrit). Elle doit se prouver par écrit au-delà de cinq mille francs.

² L'article 2015 du code civil dispose que le cautionnement ne se présume point ; qu'il doit être exprès et qu'on ne peut pas l'étendre au-delà des limites dans lesquelles il a été contracté.

Elle vous propose d'adopter l'article 4 **sans modification**.

Article 5
Application outre-mer

Cet article tend à rendre les dispositions du projet de loi applicables en Nouvelle Calédonie, en Polynésie française, à Wallis et Futuna et dans la collectivité territoriale de Mayotte. En vertu du principe de spécialité législative (article 73 de la Constitution), les lois ne sont applicables dans ces collectivités que sur mention expresse.

Votre commission des Lois¹ a approuvé plusieurs ordonnances étendant aux territoires d'outre-mer et à Mayotte les articles du code civil relatifs à la preuve testimoniale et à la preuve des actes juridiques, ainsi que l'extension à Mayotte de l'article 109 du code de commerce sur la preuve des actes de commerce.

Elle vous soumet **un amendement** rédactionnel tendant à tenir compte des évolutions statutaires actuellement en cours de discussion sur la Polynésie française, susceptible de devenir à terme un pays d'outre-mer.

Votre commission des Lois vous propose d'adopter l'article 5 **ainsi modifié**.

¹ *Rapport n° 75 (Sénat, 1999-2000) de M. Jean-Jacques Hyest portant ratification de plusieurs ordonnances portant actualisation et adaptation du droit applicable outre-mer.*

TABLEAU COMPARATIF

Texte en vigueur	Texte des propositions de loi	Texte du projet de loi	Propositions de la Commission
<p align="center">Code civil</p>			
<p><i>Livre III : Des différentes manières dont on acquiert la propriété.</i> <i>Titre III: Des contrats ou des obligations conventionnelles en général.</i> <i>Chapitre VI : De la preuve des obligations et de celle du paiement.</i></p>		<p align="center">Article 1er</p>	<p align="center">Article 1^{er}</p>
<p><i>Art. 1316</i> - Les règles qui concernent la preuve littérale, la preuve testimoniale, les présomptions, l'aveu de la partie et le serment, sont expliquées dans les sections suivantes.</p>		<p>I. - L'article 1316 du code civil devient l'article 1315-1.</p>	<p>I. - (Sans modification).</p>
<p><i>Section Ière : De la preuve littérale</i></p>		<p>II. - Les paragraphes 1er, 2, 3, 4 et 5 de la section première du chapitre VI du titre troisième du livre troisième du code civil deviennent respectivement les paragraphes 2, 3, 4, 5 et 6.</p>	<p>II. - (Sans modification).</p>
<p><i>§ 1^{er} Du titre authentique</i> <i>§ 2 De l'acte sous seing privé</i> <i>§ 3 Des tailles</i> <i>§ 4 Des copies des titres</i> <i>§ 5 Des actes reconnaissifs et confirmatifs</i></p>		<p>III. - Il est inséré, avant le paragraphe 2 de la section première du chapitre VI du titre troisième du livre troisième du code civil, un paragraphe 1er intitulé : « Dispositions générales », comprenant les articles 1316 à 1316-2 ainsi rédigés :</p>	<p>III. - (Alinéa sans modification).</p>
		<p>« <i>Art. 1316.</i> - La preuve littérale ou 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</p>	<p>« <i>Art. 1316.</i> - La preuve littérale ou <i>preuve</i> par écrit... ...transmission.</p>
	<p align="center">Proposition de loi n° 244 (1998-1999) visant à valider l'évolution</p>		

Texte en vigueur	Texte des propositions de loi	Texte du projet de loi	Propositions de la Commission
<p>Art. 1334 - Les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la représentation peut toujours être exigée.</p>	<p>jurisprudentielle en matière de preuve par écrit</p> <p>Article unique</p> <p>L'article 1334 du code civil est complété par un second alinéa ainsi rédigé :</p> <p>« Les télécopies font foi entre les parties, sous réserve, en cas de doute, d'un examen approfondi permettant d'éliminer les pièces douteuses quant à leur intégrité et à l'imputabilité de leur contenu. »</p> <p>Proposition de loi n° 246 (1998-1999) visant à reconnaître la valeur probatoire d'un message électronique et de sa signature</p> <p>Article 1er</p> <p>L'article 1334 du code civil est complété par un second alinéa ainsi rédigé :</p> <p>« Un message électronique possède une valeur probatoire sous réserve du respect de deux conditions cumulatives : d'une part, que soit possible l'authentification par une signature électronique fiable ; d'autre part, que soit assurée la conservation durable du message sous le contrôle du signataire. »</p> <p>Article 2</p> <p>Les juges pourront procéder à toutes les investigations techniques qu'ils estiment nécessaires pour établir l'authentification de la signature électronique.</p>	<p>soient leur support et leurs modalités de transmission.</p> <p>« Art. 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.</p> <p>« Art. 1316-2. - Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en</p>	<p>« Art. 1316-1. -(Sans modification).</p> <p>« Art. 1316-2. - (Sans modification).</p>

Texte en vigueur	Texte des propositions de loi	Texte du projet de loi	Propositions de la Commission
<p>Art. 1317 - L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises.</p>		<p>déterminant par tous moyens le titre le plus vraisemblable quel qu'en soit le support. »</p>	<p><i>Article additionnel</i></p> <p>« L'article 1317 du code civil est complété par un alinéa ainsi rédigé :</p> <p>« Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. »</p>
<p><i>Section I : De la preuve littérale.</i> <i>§ 2 : De l'acte sous seing privé.</i></p>		<p>Article 2</p> <p>Après l'article 1322 du code civil, il est inséré un article 1322-1 ainsi rédigé :</p> <p>« Art. 1322-1. - La même force probante est attachée à l'écrit sous forme électronique lorsqu'il constate des droits et obligations et qu'il est signé. »</p>	<p>Article 2</p> <p>« Après l'article 1316-2 du code civil, il est inséré un article 1316-3 ainsi rédigé :</p> <p>« Art. 1316-3. - L'écrit sur support électronique a la même force probante que l'écrit sur support papier, dès lors qu'il réunit toutes les conditions de forme nécessaires à sa validité. »</p>
<p>Art. 1322 - L'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a, entre ceux qui l'ont souscrit et entre leurs héritiers et ayants cause, la même foi que l'acte authentique.</p>		<p>Article 3</p> <p>Après l'article 1322-1 du code civil, il est inséré un article 1322-2 ainsi rédigé :</p> <p>« Art. 1322-2. - La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste</p>	<p>Article 3</p> <p>Après l'article 1316-3 du code civil, il est inséré un article 1316-4 ainsi rédigé :</p> <p>« Art. 1316-4. - La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le</p>

Texte en vigueur	Texte des propositions de loi	Texte du projet de loi	Propositions de la Commission
<p>Art. 1326 - L'acte juridique par lequel une seule partie s'engage envers une autre à lui payer une somme d'argent ou à lui livrer un bien fongible doit être constaté dans un titre qui comporte la signature de celui qui souscrit cet engagement ainsi que la mention, écrite de sa main, de la somme ou de la quantité en toutes lettres et en chiffres. En cas de différence, l'acte sous seing privé vaut pour la somme écrite en toutes lettres.</p>	<p>Article 3</p> <p>Les modalités de conservation durable du message électronique seront quantifiées selon les prescriptions du décret d'application de la présente proposition de loi.</p>	<p>son consentement aux obligations qui découlent de cet acte.</p> <p>« 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. »</p>	<p><i>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. »</i></p> <p><i>(Alinéa sans modification)</i></p>
		<p>Article 4</p> <p>A l'article 1326 du code civil, les mots : « de sa main » sont remplacés par les mots : « par lui-même ».</p>	<p>Article 4</p> <p><i>(Sans modification).</i></p>
		<p>Article 5</p> <p>La présente loi est applicable en Nouvelle-Calédonie, dans les territoires d'outre-mer et dans la collectivité territoriale de Mayotte.</p>	<p>Article 5</p> <p>La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans la collectivité territoriale de Mayotte.</p>

ANNEXE AU TABLEAU COMPARATIF

Code civil

Livre III : Des différentes manières dont on acquiert la propriété.

Titre III: Des contrats ou des obligations conventionnelles en général.

Chapitre VI : De la preuve des obligations et de celle du paiement.

Art. 1315 - Celui qui réclame l'exécution d'une obligation doit la prouver.
Réciproquement, celui qui se prétend libéré, doit justifier le paiement ou le fait qui a produit l'extinction de son obligation.

Art. 1316 - Les règles qui concernent la preuve littérale, la preuve testimoniale, les présomptions, l'aveu de la partie et le serment, sont expliquées dans les sections suivantes.

Section I : De la preuve littérale.

§ 1 Du titre authentique.

Art. 1317 - L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises.

Art. 1318 - L'acte qui n'est point authentique par l'incompétence ou l'incapacité de l'officier, ou par un défaut de forme, vaut comme écriture privée, s'il a été signé des parties.

Art. 1319 - L'acte authentique fait pleine foi de la convention qu'il renferme entre les parties contractantes et leurs héritiers ou ayants cause.

Néanmoins, en cas de plaintes en faux principal, l'exécution de l'acte argué de faux sera suspendue par la mise en accusation ; et, en cas d'inscription de faux faite incidemment, les tribunaux pourront, suivant les circonstances, suspendre provisoirement l'exécution de l'acte.

Art. 1320 - L'acte, soit authentique, soit sous seing privé, fait foi entre les parties, même de ce qui n'y est exprimé qu'en termes énonciatifs, pourvu que l'énonciation ait un rapport direct à la disposition. Les énonciations étrangères à la disposition ne peuvent servir que d'un commencement de preuve.

Art. 1321 - Les contre-lettres ne peuvent avoir leur effet qu'entre les parties contractantes ; elles n'ont point d'effet contre les tiers.

§ 2 De l'acte sous seing privé

Art. 1322 - L'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a, entre ceux qui l'ont souscrit et entre leurs héritiers et ayants cause, la même foi que l'acte authentique.

Art. 1323 - Celui auquel on oppose un acte sous seing privé, est obligé d'avouer ou de désavouer formellement son écriture ou sa signature.

Ses héritiers ou ayants cause peuvent se contenter de déclarer qu'ils ne connaissent point l'écriture ou la signature de leur auteur.

Art. 1324 - Dans le cas où la partie désavoue son écriture ou sa signature, et dans le cas où ses héritiers ou ayants cause déclarent ne les point connaître, la vérification en est ordonnée en justice.

Art. 1325 - Les actes sous seing privé qui contiennent des conventions synallagmatiques, ne sont valables qu'autant qu'ils ont été faits en autant d'originaux qu'il y a de parties ayant un intérêt distinct.

Il suffit d'un original pour toutes les personnes ayant le même intérêt.

Chaque original doit contenir la mention du nombre des originaux qui en ont été faits.

Néanmoins le défaut de mention que les originaux ont été faits doubles, triples, etc., ne peut être opposé par celui qui a exécuté de sa part la convention portée dans l'acte.

Art. 1326 - L'acte juridique par lequel une seule partie s'engage envers une autre à lui payer une somme d'argent ou à lui livrer un bien fongible doit être constaté dans un titre qui comporte la signature de celui qui souscrit cet engagement ainsi que la mention, écrite de sa main, de la somme ou de la quantité en toutes lettres et en chiffres. En cas de différence, l'acte sous seing privé vaut pour la somme écrite en toutes lettres.

(...)

Section II : De la preuve testimoniale.

Art. 1341 - Il doit être passé acte devant notaires ou sous signatures privées de toutes choses excédant une somme ou une valeur fixée par décret, même pour dépôts volontaires, et il n'est reçu aucune preuve par témoins contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse d'une somme ou valeur moindre.

Le tout sans préjudice de ce qui est prescrit dans les lois relatives au commerce.

(...)

Art. 1347 - Les règles ci-dessus reçoivent exception lorsqu'il existe un commencement de preuve par écrit.

On appelle ainsi tout acte par écrit qui est émané de celui contre lequel la demande est formée, ou de celui qu'il représente, et qui rend vraisemblable le fait allégué.

Peuvent être considérées par le juge comme équivalant à un commencement de preuve par écrit les déclarations faites par une partie lors de sa comparution personnelle, son refus de répondre ou son absence à la comparution.

Art. 1348 - Les règles ci-dessus reçoivent encore exception lorsque l'obligation est née d'un quasi-contrat, d'un délit ou d'un quasi-délit, ou lorsque l'une des parties, soit n'a pas eu la possibilité matérielle ou morale de se procurer une preuve littérale de l'acte juridique, soit a perdu le titre qui lui servait de preuve littérale, par suite d'un cas fortuit ou d'une force majeure.

Elles reçoivent aussi exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support.

ANNEXE 1
ÉTUDE D'IMPACT

ANNEXE 2

QU'EST-CE QUE LA SIGNATURE ÉLECTRONIQUE ?

1. Définitions.

La **signature électronique** est définie par la directive européenne comme « *une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification* ».

La **signature électronique « avancée »**, au sens de la directive, que votre commission des Lois propose de qualifier d'« élaborée », est liée uniquement au signataire, permet de l'identifier, est créée par des moyens que le signataire peut garder sous son contrôle exclusif et est liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

Elle utilise la **cryptologie**, ou cryptographie, c'est-à-dire un ensemble de techniques qui permettent de protéger les informations grâce à un code secret. Cette technique a longtemps été réglementée, en raison des intérêts qu'elle présente en matière de sécurité et de défense nationale.

En mars 1999, le Gouvernement a entrepris la **libéralisation de l'utilisation des moyens de cryptologie**¹. Désormais, l'utilisation et l'importation de moyens de cryptologie mis en œuvre par un algorithme dont la clé est d'une longueur inférieure ou égale à **40 bits** sont libres. Les logiciels de cryptologie dont la clé est d'une longueur qui ne dépasse pas **128 bits** ne sont plus soumis à autorisation, mais à une procédure de déclaration préalable.

Les logiciels de cryptologie ne prétendent pas à l'inviolabilité : si le temps n'est pas compté et que l'ordinateur est suffisamment puissant, l'algorithme peut finir par être cassé (« craqué »). Mais décrypter un message confidentiel quelques mois après qu'il a été échangé présente peu d'intérêt. En l'état actuel des techniques, il semblerait qu'il soit plus improbable de trouver une signature pour un message piraté qui soit identique à celle du message émis à l'origine que de trouver un faussaire pour imiter un tableau de maître.

¹Décret n° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.

Décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.

2. La technique des clés.

La signature électronique peut utiliser :

- une **clé symétrique**. Dans ce cas, la même clé sert à l'émetteur pour crypter¹ le message et au destinataire pour décrypter le document. Cette solution, qui nécessite un algorithme très puissant, est relativement peu satisfaisante en termes de sécurité. Mais elle présente un intérêt pour transmettre rapidement des documents de taille importante ;

- une **paire de clés** (bi-clé). Dans le système à double clé, le destinataire transmet à l'émetteur sa clé publique permettant de chiffrer le message et conserve sa clé secrète pour déchiffrer les données. La sécurité est assurée par des algorithmes spéciaux interdisant de déduire une clé à partir de l'autre clé.

Deux possibilités sont offertes :

- soit le message circule « en clair » sur le réseau Internet, mais, étant signé électroniquement, le destinataire peut vérifier que le message n'a pas été « piraté » en cours d'acheminement ;

- soit le message est crypté et signé, il circule alors sous forme inintelligible pour les tiers. Le destinataire doit le décrypter pour le rendre intelligible. Le message étant signé, le destinataire peut toujours vérifier qu'il est bien strictement identique au message initialement émis.

3. Le système de signature électronique à double clé.

L'émetteur veut envoyer un message confidentiel à un destinataire. Le destinataire veut être sûr que c'est bien l'émetteur désigné qui lui envoie le message (authentification de l'identité de l'auteur) et qu'il est le seul à pouvoir lire ce message. Pour cela, les deux correspondants vont **échanger leurs clés** de signature.

1. Le destinataire envoie sa clé publique à l'émetteur.

2. L'émetteur se sert de la clé publique du destinataire pour coder et signer le message qu'il souhaite envoyer en toute confidentialité.

3. Le destinataire vérifie la signature du message en utilisant sa clé secrète. Cette clé secrète forme un binôme inséparable avec la clé publique initialement envoyée.

La confiance entre l'émetteur et le destinataire s'établit au moment de cet échange de clés.

¹ Les termes « crypter » et « chiffrer » sont synonymes.

Les clés peuvent avoir une validité déterminée. Ainsi, l'émetteur peut confier sa clé publique à un destinataire pour une **durée limitée**.

L'utilisation du logiciel de signature est subordonnée à plusieurs **codes secrets** qui garantissent qu'une personne ayant accès à l'ordinateur de l'émetteur ne puisse utiliser la signature électronique de celui-ci.

La signature électronique s'accompagne d'un **scellement du document**. Il est impossible d'écrire deux textes différents (à une virgule près) qui aient la même signature. Le scellement permet au destinataire, en cas d'interception du message, de savoir immédiatement si le moindre caractère a été modifié par rapport au document initialement émis.

Le scellement présente ainsi un avantage considérable par rapport au support papier.

La signature permet de certifier l'auteur et le contenu du message de façon très simple pour l'utilisateur, par échange de clés publiques. Chaque binôme de correspondants a une clé commune.

La **gestion des clés** demande des compétences spécifiques. La directive européenne prévoit que ce nouveau métier sera soumis aux règles du marché intérieur, c'est-à-dire que l'activité des tiers de certification ne sera pas soumise à autorisation, mais qu'elle donnera lieu à un régime volontaire d'accréditation.

4. Exemple de transmission d'un message électronique signé.

Voici le message que l'émetteur veut envoyer :

Ceci est un message signé.

Premier cas : message signé mais non crypté.

L'émetteur veut envoyer un message non confidentiel. Il ne le crypte pas. Il utilise un logiciel de signature électronique. Il s'agit d'un logiciel spécifique, soumis à déclaration. Le message signé se présente comme suit :

-----BEGIN SIGNED MESSAGE-----

Hash: SHA1

Ceci est un message signé.

-----BEGIN SIGNATURE-----

iQA/AwUBOJg14CzrItMA4VHPEQIm4gCeKX9JVhfkJZh6DAHfWfH/hAqhYMsAn0dH
g2kNOrIg4UV71ymb/Gel9XzF=zlBq

-----END SIGNATURE-----

La signature électronique est encadrée de deux lignes marquant le commencement et la fin de la signature.

Cette technique permet de rendre impossible toute copie de la signature électronique (« copier - coller »). En d'autres termes, il n'est pas possible de copier la signature apposée en bas d'un document pour l'apposer sur un autre document. En effet, la signature résulte de la transcription, au moyen d'une fonction mathématique (algorithme), des caractères du document émis. Une signature électronique se rapporte à un texte déterminé auquel elle est indissolublement liée.

Le destinataire du document veut vérifier que c'est bien l'émetteur désigné qui le lui a envoyé. Voici comment se présente le message signé après vérification de la signature :

```
*** Signature Status: good
*** Signer: Martin DUPONT <m.dupont@senat.fr>
*** Signed: 02.02.2000 15:49:19
*** Verified: 02.02.2000 15:51:11

*** BEGIN VERIFIED MESSAGE ***
Ceci est un message signé.
*** END VERIFIED MESSAGE ***
```

Le destinataire constate qu'il s'agit bien de la signature de l'émetteur : le statut de la signature est bon (status : good), ainsi que son nom (Martin Dupont) et son adresse électronique (m.dupont@senat.fr). Cette vérification n'est possible que parce que l'émetteur a préalablement donné sa clé publique au destinataire.

La date et l'heure à laquelle a été signé le message apparaissent, ainsi que la date et l'heure à laquelle le destinataire a procédé à la vérification de la signature.

Deuxième cas : message crypté mais non signé

L'émetteur veut maintenant que son message ne circule pas « en clair » sur le réseau mais soit crypté, c'est-à-dire rendu inintelligible lors de sa transmission. Il ne signe pas son message électroniquement. L'émetteur veut envoyer ce message :

Ceci est un message crypté.

Le message crypté se présente ainsi :

```
-----BEGIN MESSAGE-----  
qANQR1DBwU4DmbRQ0aqMYzsQCAC3tFTtvUzCGINytcEkoEOOkRVYGGZdNago9tv  
10w9gG8IfvjUi5/zTX1KuPoGteKymdjiI5E6K2eGlr9msxmGlkvK6eHfoppZN87BKogati  
guBgcr85qRbG0z8K/Ow44J/DfduENSQ4F5IWRaiALst6PywvakbxY4jGm+MgWTbdiII  
95uvq21HXWCNEqcU0GEsU2eRdCKj32z+uPXF2kk8QHEjUerx7lg0u5e/DyNv52Mpy  
UbGsQweW61re5nkMY3tr9Lf27CF3/dGTVLy/xOuImA9M7ybrnzh3bWNwuKGMM6/j  
6q5HwaTIIzXUcbLuNQBV7SpmDUyG1oaBkxkxbdJz+B/wN4boMsKfvDh4JzKIvxmoG  
WWnOCXKvMQUIrNENk58cEeS4rfGywidijmbamrIk9ZtSn5G66I3CjGj4FPDdodbmecu  
Ng3733qwl0hA2SmSKDrubFBNTVj15HWVvT4a2I7nHanfffSwANy+23JNKnO7a9ns1  
Pl3w0oCacz9Few0crbvblTniCA+Kp1WWut3T92Yifq5WWKoUdcwR5QtHekrpfjvCLlh  
qGyXD5s3aHxWIQFzVUwVpWAS658IzzDTToNQsaaYBNAnlvFX3hoI/3XFSK1sfbPF  
m09nPvpree6gq9lpV3e4rW6Ki/P+5uyaMHYFBWfO9TpZyT3WqmIehli6vscyT3qOX5m  
2cSPsEQookcPr8bw4McuZAbUus+vIR4GTQXama0KkQy82muS3DloAgmJ+t2Qs7AHh  
zjmiJXRpCOC=teN7  
-----END MESSAGE-----
```

Le destinataire décrypte le message reçu en utilisant la clé publique que l'émetteur lui a préalablement remise. Il obtient le résultat suivant :

```
Ceci est un message crypté.
```

Il ne lui est pas possible de vérifier l'identité de l'émetteur ni de savoir si le message a été « piraté » au cours de sa transmission sur le réseau.

Troisième cas : message signé et crypté

Il est bien sûr possible de mixer les deux techniques. L'émetteur crypte et signe électroniquement son message. L'émetteur veut envoyer le message suivant :

```
Ceci est un message crypté et signé.
```

Le message crypté et signé se présente ainsi :

```
-----BEGIN MESSAGE-----  
qANQR1DBwU4DmbRQ0aqMYzsQCAC5YNnwfCjeV4nT/no0DNK/S102Q6C6yp5/J7R  
HZwnnaZnMoBzNgh8HuXgwq/Vu6gHtE9ownDnH5kU5+PX9Udn9lLw5jPtYos4E540Jd  
3HscB/waBxLeZhJ4i09ejCgKSOHEOrvkNxep8Ls/KW13HrKQ22UPsf+OhCZV75vH3  
By+G7Wb1DSSqW6LI8di01D7WIwfWws3IPf6cKoSlswYjQTMqkxKPRmLkX0IvhFJy  
L8R5/ULqC4fwb8VvSHw7jVyhoPlfCMn2DidOYgCTbv4UUg2Xm709GlbTM5VPHtm  
HG61B6VhwcuEUMM+5ZMPq6vcj2pICczygJ7nrFwUz6R8bs4CAC1VTrEn4oIy99Bv  
N9zi64UGPGMI8IKTT7J7fXDlv/hg6JcdlSSbb+o5MPFE7urbU4rYwIYz3cEXz9GftkkC  
2dQv4v+TU3Ba8WTnm2kAjO3UPkdQm1iRh6YNrLuHgiJKrj7BUbSoRrv6qgP4HsGH9  
PzpjRO5K60Nx/7LsWAI93/o5Mz/YK/p4HJi6gA/BQYxK4G3SCBb9/280v/Tv6bY9aX  
HtBAqktXoxq6GjliHzGria6rWbOtVhrRwMqKNx48ZLLjn7CPm9iBtqWEGMksC8nVS
```

```
W2pW4R2GKdpAPOuiRD/vfL2p7Zbf68g7fLsB4kxdiSaklCQq8AJxLcgHzukiOdVyZVn
5SooExMbMjZkGIgSKURUWPJWw9I9nuxxUdTX9G6SgHd7KoCmnWeiAjE7AgBMF
YH6NeCIFQI92ShK3kRkfx+JIxB9hHkCU8LAXjqEiCEfobOQPFLBv6O6ceYwVmZjkR
mQKYZNM0bWZhWOEbIqnlbKUUGVEOFaYeKoqpt8RFzuS+xsH99FYKBSchHgWze
uVzGFIfooWA===HWMa
```

-----END MESSAGE-----

Le destinataire décrypte le message et sa signature. Il obtient le résultat suivant :

```
*** Signature Status: good
*** Signer: Martin DUPONT <m.dupont@senat.fr>
*** Signed: 02.02.2000 16:01:18
*** Verified: 02.02.2000 16:04:51

*** BEGIN DECRYPTED/VERIFIED MESSAGE ***

Ceci est un message crypté et signé.

*** END DECRYPTED/VERIFIED MESSAGE ***
```

Quatrième cas : le message signé a été « piraté ».

L'émetteur veut envoyer le message signé suivant :

Message signé dont le contenu est modifié.

Ce message a été intercepté lors de sa transmission sur le réseau. Le « pirate » en modifie le contenu. Il rajoute la phrase suivante :

Texte rajouté après la création de la signature.

Le « pirate » renvoie le message ainsi modifié au destinataire. Le destinataire reçoit ceci :

```
*** Signature Status: bad
*** Signer: Martin DUPONT <m.dupont@senat.fr>
*** Signed: 03.02.2000 16:20:59
*** Verified: 03.02.2000 16:21:50

*** BEGIN VERIFIED MESSAGE ***

Message signé dont le contenu est modifié.
Texte rajouté après la création de la signature.

*** END VERIFIED MESSAGE ***
```

Le destinataire s'aperçoit tout de suite que le message a été intercepté (status : bad). Il ne doit pas faire confiance au contenu du message.

La modification directe de la signature empêche sa vérification par le programme (message d'erreur), ce qui signale son invalidité.

Le fonctionnement est identique pour un message crypté.

ANNEXE 3

LES « AMENDEMENTS ÉLECTRONIQUES » AU SÉNAT

Comme l'a souligné le président Christian Poncelet dans son allocution du 7 octobre 1998, l'utilisation des nouvelles technologies constitue un élément indispensable à la modernisation des méthodes de travail du Sénat. Une réflexion a donc été engagée sur la **dématérialisation de la chaîne législative**, depuis le dépôt du projet de loi jusqu'à son adoption définitive.

1. Le dépôt des amendements par voie électronique

Le dépôt électronique des amendements des sénateurs, en vue de leur discussion en séance publique, prend deux formes :

- les amendements des commissions¹ sont directement transmis au service de la Séance par le réseau informatique interne du Sénat ;

- depuis juin 1998, les amendements peuvent être adressés par chaque sénateur au service de la Séance par la voie de la messagerie électronique à une adresse spécifique : « amendements@sénat.fr ».

Aujourd'hui, **environ 60 % des amendements sont déposés sous forme électronique**, l'objectif étant d'aboutir à terme à une transmission électronique de la totalité des amendements.

Au début du mois de janvier 2000, le Conseil de Questure et le Bureau sur le rapport de M. le Questeur délégué François Autain, ont autorisé le lancement d'une procédure d'appel d'offres en vue de la réalisation d'un projet d'informatisation de la chaîne des amendements dit projet AMELI (Amendements En Ligne).

Ce projet permettra le dépôt des amendements par la voie du site Internet et la mise à disposition de tous les intervenants au processus législatif d'un jeu des amendements permettant des consultations sélectives. Ainsi, tout parlementaire, qu'il se trouve dans le Palais ou dans son département, le Gouvernement ou toute personne intéressée, sera en mesure de connaître en temps réel le nombre, l'origine ou le texte des amendements déjà déposés sur chaque article.

¹ Le Sénat, comme l'Assemblée nationale, comprend six commissions permanentes (article 43 de la Constitution). Il s'agit des commissions des affaires culturelles, des affaires économiques, des affaires étrangères, des affaires sociales, des finances et des lois.

La mise en œuvre de ces nouvelles possibilités de dépôt des amendements supposait de **lever deux préalables**, tenant d'une part aux contraintes de la procédure parlementaire, et d'autre part aux caractéristiques propres de la messagerie électronique :

- la vérification du respect du **délai-limite** imparti aux sénateurs pour remettre les amendements au service de la Séance ;

- la **valeur probatoire** à accorder aux amendements parvenus par messagerie électronique.

A la première question, il a été répondu que l'heure de réception du message par le serveur de la messagerie du Sénat ferait foi.

S'agissant de la valeur probatoire des amendements, le mode de dépôt traditionnel, c'est-à-dire la transmission physique par le sénateur, de la version papier signée des amendements, **évite toute incertitude quant à l'auteur de l'amendement et à l'heure de sa réception.**

Dès lors, comment la transmission électronique des amendements peut-elle offrir les mêmes garanties, notamment lors de la transmission d'amendements depuis l'extérieur du Palais du Luxembourg par l'intermédiaire de prestataires d'accès externes ?

Pour l'instant, une alerte par la voie d'un appel téléphonique préalable du service de la Séance permet au sénateur auteur de l'amendement de s'assurer que l'envoi est bien parvenu. En retour du dépôt, un avis de réception électronique est adressé, à titre de confirmation par le service de la Séance.

2. Les questions des sénateurs

Les questions écrites ou orales sans débat adressées par les sénateurs aux ministres peuvent être déposées par messagerie électronique dans les mêmes conditions depuis octobre 1998.

Cette nouvelle faculté s'ajoute aux modes plus traditionnels de dépôt des questions, par courrier et par fax.

3. Les propositions de loi ou de résolution

Dans la même optique a été ouverte depuis le début de l'année 2000 la possibilité pour les sénateurs de déposer leurs propositions de loi ou de résolution par la voie de la messagerie électronique à l'adresse suivante : « propositions@sénat.fr ».

Cette nouvelle possibilité permettra non seulement d'effectuer une distribution plus rapide des propositions mais également d'assurer leur mise en

ligne immédiate sur le site Internet du Sénat ce qui n'était pas le cas jusqu'à présent.

*

* *

La signature électronique définie par le présent projet de loi est de nature à répondre aux exigences de la transmission par voie électronique des amendements : elle permet d'authentifier l'auteur de l'amendement ; elle manifeste son consentement au contenu de l'amendement.

ANNEXE 4

LES DOCUMENTS DE TRAVAIL DU SENAT

Série **LEGISLATION COMPAREE**

LA SIGNATURE ELECTRONIQUE

n° LC 67 - Décembre 1999

Ce document constitue un instrument de travail élaboré à l'intention des Sénateurs par la Division des études de législation comparée du Service des affaires européennes. Il a un caractère informatif et ne contient aucune prise de position susceptible d'engager le Sénat.

Le projet de loi français portant adaptation du droit de la preuve aux nouvelles technologies de l'information et relatif à la signature électronique tend à introduire une présomption de fiabilité au profit des signatures électroniques qui répondent à certaines conditions, lesquelles devront être précisées par décret en Conseil d'Etat.

Ce projet amène à s'interroger sur le régime juridique de la signature électronique chez nos principaux voisins. La présente étude couvre plusieurs pays européens (**Allemagne, Belgique, Danemark, Espagne, Italie, Luxembourg et Royaume-Uni**). Pour chacun de ces pays, elle vérifie si la signature électronique bénéficie de la reconnaissance législative et en analyse les effets juridiques. Elle examine ensuite, le cas échéant, les conditions de validité de la signature électronique. La **directive européenne sur un cadre communautaire pour les signatures électroniques**, adoptée le 30 novembre 1999, a également été étudiée, et les conditions de validité de la signature électronique dans les différents pays sous revue - qu'elles s'appliquent déjà ou qu'elles ne soient que prévues - ont été comparées aux dispositions prises au niveau européen.

L'examen de la situation dans ces sept pays fait apparaître que :

- **l'Allemagne et l'Italie sont actuellement les seuls pays où un texte définit le régime juridique de la signature électronique ;**
- **les textes allemand et italien ne reconnaissent que certaines formes de signature électronique et leur accordent des effets différents ;**

- les projets espagnol et luxembourgeois, ainsi que les avant-projets anglais, belge et danois, visent toutes les formes de signature électronique, mais ils divergent dans les effets qu'ils leur reconnaissent.

Qu'est-ce que la signature électronique ?

Le développement du commerce électronique est subordonné à l'existence de garanties sur la sécurité des transmissions de données et des paiements en ligne. Grâce à un système de chiffrement appliqué au message transmis, sans que ce dernier soit nécessairement lui-même chiffré, la signature électronique constitue une réponse au problème, car elle garantit l'authenticité et l'intégrité des données, ainsi que l'identité du signataire. Si la confidentialité est requise, il faut chiffrer le contenu du message.

De façon générale, le chiffrement consiste à rendre le texte d'un message illisible pour qui ne détient pas la clé de déchiffrement. Dans les systèmes de chiffrement symétriques, une seule clé sert à la fois à chiffrer et à déchiffrer les données. Elle doit être gardée secrète par les parties intéressées pour que la sécurité de l'information soit garantie. L'inconvénient principal réside dans le fait que l'expéditeur et le destinataire doivent convenir à l'avance de la clé et doivent disposer d'un canal sûr pour l'échanger.

C'est pourquoi **les systèmes de signature électronique qui se développent depuis quelques années reposent sur des algorithmes de chiffrement asymétriques, où, de plus, chaque utilisateur dispose de deux clés, une clé publique et une clé privée. Ces deux clés sont elles-mêmes créées à l'aide d'algorithmes mathématiques. Elles sont associées l'une à l'autre de façon unique et sont propres à un utilisateur donné.** Un message chiffré à l'aide d'un algorithme asymétrique et d'une clé privée, qui constitue l'un des paramètres de l'algorithme, ne peut être déchiffré qu'avec la clé publique correspondante, et inversement. **La clé publique doit donc être connue de tous, tandis que la clé privée reste secrète,** la carte à puce semblant être le meilleur support de stockage des clés privées. Lorsque l'algorithme de chiffrement asymétrique est utilisé seulement pour créer la signature électronique, les mêmes clés, privée et publique, sont utilisées, mais seulement pour vérifier l'authenticité et l'intégrité du message.

Ces signatures électroniques, obtenues par l'application d'algorithmes asymétriques, sont parfois qualifiées de numériques ou de « digitales », par opposition aux signatures électroniques créées au moyen d'autres dispositifs.

Selon la Commission des Nations Unies pour le droit commercial international, une signature numérique est *« une valeur numérique apposée à un message de données et qui, grâce à une procédure mathématique bien connue associée à la clé cryptographique privée de l'expéditeur, permet de déterminer que cette valeur numérique a été créée à partir de la clé cryptographique privée de l'expéditeur. Les procédures mathématiques utilisées pour créer les signatures numériques sont fondées sur le chiffrement de la clé publique. Appliquées à un message de données, ces procédures mathématiques opèrent une transformation du message de telle sorte qu'une personne disposant du message initial et de la clé publique de l'expéditeur peut déterminer avec exactitude : a) si la transformation a été opérée à l'aide de la clé privée correspondant à celle de l'expéditeur ; et b) si le message initial a été altéré une fois sa transformation opérée (...) »*

Contrairement à la signature manuscrite, la signature numérique, composée de chiffres, de lettres et d'autres signes, **ne comporte aucun élément permettant de l'attribuer à une personne donnée.** Chaque utilisateur doit donc établir avec certitude l'identité de ses correspondants. C'est pourquoi on recourt à des **services de certification**, souvent désignés comme « tiers de certification », qui disposent de la confiance de chacun et qui garantissent l'appartenance d'une signature à une personne. Comme le destinataire utilise la clé publique de l'expéditeur pour vérifier la signature électronique de ce dernier, la vérification suppose que le tiers certifie au destinataire que la clé publique qu'il utilise correspond bien à la clé privée de l'expéditeur signataire et que ce dernier est bien celui qu'il prétend être. Les tiers de certification délivrent donc des **certificats d'authentification** qui contiennent, d'une part, divers renseignements sur la personne dont on souhaite vérifier l'identité (nom, prénom, date de naissance...) et, d'autre part, sa clé publique. Ces certificats sont généralement réunis dans des bases de données mises en ligne sur le réseau Internet, ce qui permet à chacun d'y accéder facilement.

La signature numérique constitue donc un bloc de données créé à l'aide d'une clé privée ; la clé publique correspondante et le certificat permettent de vérifier que la signature provient

réellement de la clé privée associée, qu'elle est bien celle de l'expéditeur et que le message n'a pas été altéré.

1) Seules l'Allemagne et l'Italie disposent de textes sur la signature électronique, mais des législations sont en préparation dans les autres pays

a) Depuis 1997, le régime juridique de la signature électronique est déterminé par une loi en Allemagne et par un décret en Italie

En effet, l'Allemagne a adopté en juin 1997 la loi sur la signature « digitale », qui constitue en fait la troisième partie d'une loi générale sur la société de l'information et qui a été complétée par une ordonnance entrée en vigueur le 1^{er} novembre 1997.

En Italie, un décret du Président de la République, pris en 1997 en application de la loi Bassanini sur la réforme de l'administration publique, définit le régime juridique des documents informatiques, parmi lesquels la signature électronique. Les dispositions de ce décret qui concernent cette dernière ont été précisées au début de l'année 1999 par un décret du Président du conseil.

b) Dans chacun des autres pays, un projet de loi est actuellement en préparation ou en discussion

En Belgique, le gouvernement en fonction jusqu'aux élections législatives de juin 1997 avait adopté deux projets de loi : l'un visant à modifier certaines dispositions du code civil sur la preuve des obligations et l'autre concernant les tiers de certification. Seul le premier avait été déposé au Parlement, mais il est devenu caduc. Le gouvernement actuel a préparé un projet sur les tiers de certification, mais il ne l'a pas encore déposé au Parlement.

Le projet de loi danois sur la signature électronique est en cours d'élaboration. Un premier avant-projet de loi avait été rédigé au début de l'année 1998 et les parties intéressées avaient été consultées. Cependant, les désaccords entre les ministères de la Recherche et de la Justice ont conduit le gouvernement à attendre l'adoption de la directive pour rendre public un nouvel avant-projet de loi. De même, au Royaume-Uni, l'avant-projet de loi sur les moyens électroniques de communication, qui définit notamment le régime juridique de la signature électronique, a été rendu public en juillet 1999, et le projet de loi devrait être déposé au début de l'année 2000.

En revanche, en Espagne, le projet de loi sur la signature électronique est actuellement soumis à la commission compétente du Congrès

des députés. Il devrait être adopté au cours des premières semaines de l'année 2000. Au Luxembourg, les dispositions relatives à la signature électronique font partie d'un projet plus large, qui concerne le commerce électronique et qui a déjà été déposé au Parlement.

2) Les textes allemand et italien ne reconnaissent que certaines formes de signature électronique et leur accordent des effets différents

a) La loi allemande et le décret italien ne traitent que de la signature électronique fondée sur un système de chiffrement asymétrique

Le domaine d'application des deux textes est limité aux signatures numériques, c'est-à-dire aux signatures électroniques créées à l'aide d'un procédé de chiffrement asymétrique.

Aucun de ces textes n'évoque les autres signatures électroniques, dont la valeur est donc laissée à l'appréciation du juge.

b) Les deux textes n'accordent pas les mêmes effets juridiques à la signature numérique

Le décret italien confère à la signature numérique les mêmes effets juridiques qu'à la signature manuscrite et prévoit qu'elle puisse remplacer n'importe quel signe, sceau, cachet, poinçon... Il prévoit même que, à l'image de la signature manuscrite, elle puisse être authentifiée par un officier ministériel.

En revanche, **la loi allemande ne contient aucune disposition explicite sur la recevabilité en justice et sur la valeur probante de la signature numérique.** Elle ne remet pas non plus en cause la liberté qu'a le juge d'apprécier les éléments de preuve qui lui sont soumis. Elle définit seulement les conditions dans lesquelles le destinataire peut être sûr de l'identité de l'émetteur et de l'intégrité des données transmises. Il paraît donc probable que, sauf dans les cas où une signature manuscrite est expressément exigée, le juge admettra la valeur probante des signatures numériques.

3) Les projets de loi espagnol et luxembourgeois, ainsi que les avant-projets anglais, belge et danois, visent toutes les formes de signature électronique, mais divergent dans les effets qu'ils leur reconnaissent

a) Les cinq projets s'appliquent à toutes les formes de signature électronique, indépendamment de la technologie retenue...

Reprenant plus ou moins fidèlement la formulation de la directive, les cinq textes définissent la signature électronique comme une donnée électronique qui sert de méthode d'authentification. Même s'ils paraissent avoir été rédigés pour s'appliquer aux signatures électroniques créées grâce à un procédé de chiffrement asymétrique, ils n'excluent *a priori* aucune autre forme de signature électronique et respectent donc le principe de neutralité technologique qui sous-tend la directive.

Malgré ce principe, certains textes ne sont pas destinés à s'appliquer à toutes les signatures électroniques. En effet, l'avant-projet de loi belge ne traite que de la signature électronique « avancée », c'est-à-dire la signature électronique produite grâce à un dispositif qui est lié de manière unique et certaine au signataire et qu'il peut garder sous son contrôle exclusif. Il en va de même de l'avant-projet danois, qui, sans se référer explicitement à la signature électronique « avancée », ne s'applique qu'aux signatures électroniques les plus fiables.

Par ailleurs, à l'image de la directive, les projets de lois espagnol et luxembourgeois établissent une distinction en fonction du degré de fiabilité des signatures électroniques : ils opposent en effet la signature électronique et la signature électronique « avancée ».

b) ... sans leur reconnaître la même valeur juridique

Comme la directive, les projets belge, espagnol et luxembourgeois considèrent comme **équivalentes aux signatures manuscrites les signatures électroniques créées dans des conditions de sécurité optimales**, c'est-à-dire les signatures électroniques « avancées » qui, de plus, sont associées à un certificat particulièrement fiable et sont créées par un dispositif sécurisé. En revanche, ils ne reconnaissent aucun effet juridique particulier aux autres signatures électroniques. Cependant, les projets espagnol et luxembourgeois précisent explicitement, tout comme la directive, qu'elles seront recevables en justice.

Les avant-projets de loi anglais et danois ne comportent pas la notion de signature électronique « avancée ». Le premier prévoit, de façon générale, la recevabilité des signatures électroniques, quelles qu'elles soient, mais laisse au juge le soin d'apprécier leur valeur probante, tandis que le second détermine seulement les conditions dans lesquelles les signatures électroniques peuvent être considérées comme sûres, sans remettre en cause la totale liberté du juge pour évaluer leur recevabilité et leur valeur probante.

* *

*

Outre ces divergences importantes dans son régime même, il faut souligner que les conditions de validité de la signature électronique, notamment celles qui se rapportent aux tiers de certification, sont assez différentes d'un pays à l'autre.

Ainsi, la loi allemande et le décret italien ne contiennent aucune disposition sur leur responsabilité. Il en va de même de l'avant-projet de loi anglais, qui est particulièrement libéral.

En effet, conformément aux recommandations de la commission parlementaire, il laisse les professionnels mettre en place un dispositif d'accréditation, alors que tous les autres textes, en vigueur ou en préparation, définissent un système d'accréditation obligatoire, au moins pour les tiers de certification qui délivrent les certificats les plus fiables.

LA SIGNATURE ELECTRONIQUE

UNION EUROPEENNE

Le 13 mai 1998, la Commission a présenté la **proposition de directive sur un cadre commun pour les signatures électroniques**.

Le Parlement européen l'a approuvée le 13 janvier 1999, après avoir introduit quelques amendements. La Commission a donc présenté une proposition modifiée le 29 avril 1999, sur laquelle le Conseil a adopté une position commune. Le 27 octobre 1999, le Parlement européen a adopté quelques amendements formels à ce texte, sur lequel le Conseil s'est prononcé le 29 novembre 1999 (document n° 1).

1) LA RECONNAISSANCE JURIDIQUE DE LA SIGNATURE ÉLECTRONIQUE

L'article premier de la directive énonce : « *L'objectif de la présente directive est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique (...)* ».

A l'article suivant, elle définit **deux niveaux de signature électronique**. Elle distingue en effet la « signature électronique », qu'elle qualifie de « *donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification* », de la « signature électronique avancée », qui doit en outre satisfaire aux exigences suivantes :

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

2) LES EFFETS JURIDIQUES DE LA SIGNATURE ÉLECTRONIQUE

D'après la directive, **seules les signatures électroniques créées dans des conditions de sécurité optimale peuvent avoir la même valeur que les**

signatures manuscrites. En effet, cette équivalence est réservée aux signatures électroniques avancées « *basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature* ».

Toutefois, **les autres signatures électroniques doivent pouvoir être reconnues en justice.** Le seul fait qu'elles ne reposent pas sur un certificat qualifié, que le certificat n'ait pas été délivré par un tiers de certification agréé, ou qu'elles ne résultent pas d'un dispositif sécurisé de création de signature ne doit pas empêcher *a priori* qu'elles soient reçues comme preuves.

3) LES CONDITIONS DE VALIDITÉ DE LA SIGNATURE ÉLECTRONIQUE

La recevabilité en justice des signatures électroniques et la qualification de signature électronique « avancée », reposent sur des conditions relatives :

- aux certificats ;
- aux tiers de certification ;
- au processus de création de la signature électronique.

a) Les certificats

Les titulaires des certificats sont des **personnes physiques** qui peuvent, le cas échéant, agir pour le compte d'une personne morale. La directive ne mentionne aucune indication de durée de validité maximale pour les certificats.

L'annexe I de la directive énumère les exigences relatives aux certificats « qualifiés ». Ces derniers comportent nécessairement :

« a) *une mention indiquant que le certificat est délivré à titre de certificat qualifié ;*

« b) *l'identification du prestataire de service de certification, ainsi que le pays dans lequel il est établi ;*

« c) *le nom du signataire ou un pseudonyme qui est identifié comme tel ;*

« d) *la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat est destiné ;*

« e) *des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire ;*

» f) l'indication du début et de la fin de la période de validité du certificat ;

» g) le code d'identité du certificat ;

» h) la signature électronique avancée du prestataire de service de certification qui délivre le certificat ;

» i) les limites à l'utilisation du certificat, le cas échéant ; et

» j) les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant ».

b) Les tiers de certification

Si la fourniture de services de certification ne peut être soumise à une autorisation préalable, et peut être assurée par toute personne physique ou morale, les Etats membres doivent cependant instaurer un système de contrôle des tiers de certification. La directive prévoit par ailleurs que les Etats membres puissent, pour « améliorer le niveau du service de certification fourni », instaurer un système d'accréditation.

L'annexe II de la directive définit les exigences concernant les tiers de certification qui délivrent des certificats agréés.

« Les prestataires de service de certification doivent :

» a) faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification ;

» b) assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat ;

» c) veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision ;

» d) vérifier, par des moyens appropriés et conformes au droit national, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré ;

» e) employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées ; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues ;

» f) 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 ;

» g) prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données ;

» h) disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente directive, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée ;

» i) enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier, pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques ;

» j) ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés ;

» k) avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information, qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat ;

» l) utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable, de sorte que :

- seules les personnes autorisées puissent introduire et modifier des données,

- l'information puisse être contrôlée quant à son authenticité,

- les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement, et

- toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur. »

La directive prévoit la responsabilité des tiers de certification pour tout préjudice causé par l'utilisation d'un certificat inexact ou invalide. Ils peuvent cependant dégager leur responsabilité en prouvant qu'ils n'ont commis aucune négligence.

c) Le dispositif de création de la signature électronique

Les dispositifs sécurisés de création de signature sont définis à l'annexe III de la directive :

« 1. Les dispositifs sécurisés de création de signature doivent au moins garantir, par les moyens techniques et procédures appropriés, que :

» a) les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée ;

» b) l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles ;

» c) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

» 2. Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature ».

LA SIGNATURE ELECTRONIQUE

ALLEMAGNE

1) LA RECONNAISSANCE LÉGISLATIVE DE LA SIGNATURE ÉLECTRONIQUE

La loi fédérale établissant les conditions générales pour les services d'information et de communication, adoptée le 13 juin 1997, comprend plusieurs parties. La troisième correspond à la **loi sur la signature « digitale »** (document n° 2), qui est entrée en vigueur le 1^{er} août 1997. Une **ordonnance** (document n° 3), entrée en application le 1^{er} novembre 1997, précise les conditions de mise en œuvre de cette loi.

L'article 1^{er} de la loi sur la signature « digitale » définit l'objet de la loi, qui est *« de poser les conditions générales auxquelles sont soumises les signatures digitales pour être considérées comme sûres et pour que les faux en signature digitale ou la manipulation des données puissent être établis de manière fiable »*.

La loi sur la signature « digitale » définit donc les **conditions techniques d'une transmission fiable des données électroniques**, pour que le destinataire soit sûr de l'identité de l'émetteur et de l'intégrité des données transmises.

Elle ne traite que de la signature « digitale », qui est fondée sur la cryptographie asymétrique et qu'elle définit à l'article 2 comme : *« un sceau attaché à une donnée numérique qui est produit par une clé privée, qui authentifie le propriétaire de la clé et établit l'intégrité des données au moyen d'une clé publique correspondante fournie avec un certificat de clé, lequel est délivré par un prestataire de service de certification ou par l'autorité de contrôle »*.

2) LES EFFETS JURIDIQUES DE LA SIGNATURE ÉLECTRONIQUE

La loi ne **contient aucune disposition explicite sur la recevabilité en justice et sur la valeur probante de la signature « digitale »**. Elle ne remet pas non plus en cause le principe selon lequel le juge apprécie librement la force probante des éléments qui lui sont soumis.

Le code de procédure civile reconnaît cinq moyens de preuve, parmi lesquels « l'observation ». Or, la jurisprudence admet depuis plusieurs années que « l'observation » ne se limite pas à l'observation visuelle et qu'elle peut s'appliquer à des documents informatiques.

Comme le juge apprécie librement la valeur probante des éléments qui lui sont soumis et que la loi garantit la fiabilité des signatures « digitales », parce qu'elles répondent aux critères qu'elle-même définit et que l'ordonnance précise, il paraît probable que les signatures « digitales » seront reconnues comme moyen de preuve, sauf dans les cas où la loi exige une signature manuscrite.

Le législateur allemand a souhaité pouvoir faire un bilan de la mise en œuvre de la loi avant de reconnaître une équivalence entre la signature « digitale » et la signature manuscrite, conformément à l'article 5 de la directive. Cependant, le ministère de la Justice a déjà publié une note dans laquelle il propose que, pour certains actes juridiques requérant une signature manuscrite, l'équivalence soit reconnue.

Depuis le 1^{er} janvier 1999, **un règlement administratif relatif à la comptabilité en matière de sécurité sociale autorise la signature « digitale »** dans la mesure où elle est conforme à la réglementation en vigueur.

3) LES CONDITIONS DE VALIDITÉ DE LA SIGNATURE ÉLECTRONIQUE

La qualification de signature « digitale » dépend du respect de conditions relatives :

- aux certificats ;
- aux tiers de certification ;
- au processus de création de la signature électronique.

a) Les certificats

L'article 2 de la loi définit le **titulaire** du certificat comme une **personne physique**.

Il prévoit, outre le certificat de clé, le **certificat d'attribution**, qui est « *un certificat électronique séparé contenant de plus amples informations et qui fait expressément référence à un certificat de clé spécifique* ».

L'article 7 de la loi, qui indique les informations que doit contenir le certificat de clé, ne correspond pas totalement aux exigences concernant les certificats « qualifiés » et figurant à l'annexe I de la directive.

La durée de validité des certificats ne peut excéder cinq ans.

b) Les tiers de certification

La loi régleme l'activité des tiers de certification en instaurant **des licences, qui sont délivrées par une autorité de contrôle**. Il s'agit de l'**Autorité de régulation pour les télécommunications et la poste**, mise en place par la loi sur les télécommunications du 25 juillet 1996, et dont les membres sont désignés par le gouvernement fédéral, le Bundestag et le Bundesrat.

La loi n'interdit pas explicitement l'activité de tiers de certification non accrédités, mais cette activité se déroule alors en dehors du cadre de la loi. Les signatures associées ne bénéficient donc pas de la garantie de fiabilité définie par la loi.

Cet organisme veille également à ce que les tiers de certification respectent l'ensemble de la réglementation. Elle est aidée, pour les vérifications techniques, par des organismes (un public et trois privés) qu'elle désigne et qui lui rendent compte de façon très détaillée.

L'article 4 de la loi et l'article 1^{er} de l'ordonnance précisent les conditions que doivent remplir les tiers de certification et les obligations qu'ils doivent respecter. Elles sont analogues aux exigences posées par l'annexe II de la directive. En revanche, **le législateur n'a pas introduit de dispositions spécifiques relatives à la responsabilité des tiers de certification**, faute d'être parvenu à un consensus.

La loi impose aux tiers de certification le respect de **mesures de sécurité et de dispositions d'ordre technique assorties de conditions qualitatives très strictes**. L'article 14 décrit les composants techniques qui doivent être utilisés, notamment pour la production et l'archivage des clés, ainsi que pour la production et la vérification des signatures « digitales ». Des précisions sont apportées dans l'ordonnance par les articles 16 et 17. Ce dernier article fait référence à des normes techniques particulièrement précises. Ces dispositions ont été elles-mêmes complétées par la publication, en 1998, par l'Autorité de régulation pour les télécommunications et la poste, de deux catalogues de mesures techniques rédigés selon les conseils du Bureau fédéral pour la sécurité dans la technique d'information.

L'article 8 de l'ordonnance oblige le prestataire de service de certification à conserver les certificats qu'il a délivrés dans un **registre public**. Le certificat doit figurer au registre au moins pendant la durée de qualification de l'algorithme et des paramètres pertinents utilisés. L'Autorité de régulation pour les télécommunications et la poste publie la liste des algorithmes et paramètres pertinents qualifiés avec leur durée de validité. Celle-ci doit être d'au moins six ans, sauf problème particulier.

L'article 13 de l'ordonnance précise que **l'ensemble des informations relatives aux mesures de sécurité et aux certificats doit être gardé au moins trente-cinq ans** à compter de l'émission du certificat de clé et archivé de manière à être consultable à tout moment pendant cette période.

L'article 5 de l'ordonnance **interdit l'archivage des clés privées par l'autorité de certification**.

c) Le dispositif de création de la signature électronique

L'article 6 de l'ordonnance prévoit que le tiers de certification transmet la clé privée et les données d'identification **au signataire en personne, qui en accuse réception par écrit**. Dès cet instant, elles sont **sous la garde personnelle du signataire**.

En pratique, c'est une carte à puce qui contient la clé privée et les autres paramètres nécessaires à la création de la signature « digitale ». Le document électronique est signé en introduisant cette carte dans un lecteur spécial branché sur l'ordinateur et en tapant un code secret.

LA SIGNATURE ELECTRONIQUE

BELGIQUE

1) LA RECONNAISSANCE LÉGISLATIVE DE LA SIGNATURE ÉLECTRONIQUE

Le gouvernement en fonction jusqu'aux élections législatives de juin 1999 avait déposé au Parlement, le 14 avril 1999, un projet de loi visant à modifier certaines dispositions du code civil relatives à la preuve des obligations, parmi lesquelles l'article 1322 relatif à la valeur probante des actes sous seing privé. Le projet introduisait une définition fonctionnelle de la signature et disposait que celle-ci pouvait être « *un ensemble de données numériques pour autant qu'elle puisse être imputée à une personne déterminée et qu'elle établisse le maintien de l'intégrité de l'acte* ». En reconnaissant une équivalence probatoire entre la signature manuscrite et la signature électronique, il transposait partiellement la directive et devait être complété par un autre projet sur les tiers de certification. Ce dernier avait été adopté en conseil des ministres, mais n'avait pas été déposé au Parlement.

Le gouvernement actuel n'a pas repris le texte déposé, qui est donc devenu caduc, et a choisi d'élaborer un **projet de loi sur l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques** (document n° 4). Approuvé par le Conseil d'Etat, le projet de loi doit être signé par le Roi avant d'être déposé au Parlement.

Cet avant-projet de loi a pour objet de : « *fixer les conditions générales d'accréditation des prestataires de services de certification (...) afin de renforcer la sécurité et la confiance dans l'utilisation de la signature électronique avancée en réseaux ouverts* ».

Ce **projet de loi ne vise que la signature électronique avancée**, dont la définition, mentionnée à l'article premier, reprend celle de la directive.

2) LES EFFETS JURIDIQUES DE LA SIGNATURE ÉLECTRONIQUE

L'avant-projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation des signatures électroniques reconnaît à certaines signatures électroniques créées dans des conditions de sécurité optimales la même force probante qu'à une signature manuscrite.

En effet, l'article 4-4 de ce texte prévoit « *qu'une signature électronique avancée réalisée sur la base d'un certificat qualifié et créé par un dispositif sécurisé de création de signature est assimilée à une signature au sens de l'article 1322 du code civil* ».

Cette catégorie de signatures électroniques avancées bénéficierait d'une assimilation automatique à une signature manuscrite. Leur valeur probante s'imposerait au juge.

En revanche, la valeur des autres signatures électroniques continuerait à être librement appréciée par le juge.

Il convient par ailleurs de rappeler que, en matière civile, l'article 1341 du code civil prévoit qu'« *il doit être passé acte devant notaire ou sous signature privée, de toutes choses excédant une somme ou une valeur de 15 000 F* », (c'est-à-dire 2 500 FRF). Par conséquent, le juge civil est en mesure de rejeter un document au seul motif qu'il est signé électroniquement.

* *

*

La signature électronique est **actuellement reconnue dans le secteur de la sécurité sociale** par l'**arrêté royal du 11 avril 1999**, qui prolonge **jusqu'au 30 juin 2000** l'application de l'arrêté royal du 16 octobre 1998 portant dispositions relatives à la signature électronique, lequel s'applique à la sécurité sociale, conformément à l'article 38 de la loi du 26 juillet 1976 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux de pension. Ainsi, certaines déclarations d'emploi sont signées électroniquement au moyen de certificats numériques proposés par des autorités de certification accréditées par la Banque Carrefour de la sécurité sociale, qui est l'organisme chargé de collecter, pour le compte de toutes les institutions de sécurité sociale, les informations relatives aux assurés sociaux et aux employeurs.

Par ailleurs, en septembre 1998, les administrations fédérales belges ont achevé de rédiger un protocole d'accord : *Agora ou l'infrastructure nécessaire à l'utilisation de la signature électronique par les administrations fédérales*.

3) LES CONDITIONS DE VALIDITÉ DE LA SIGNATURE ÉLECTRONIQUE

L'avant-projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques prévoit que les effets juridiques de la signature électronique avancée dépendent du respect de conditions relatives :

- aux certificats ;

- aux tiers de certification ;
- au processus de création de la signature électronique.

a) Les certificats

Le texte traite du seul **certificat « qualifié »**, qui est fourni par un prestataire de service de certification accrédité et qui doit contenir les informations obligatoires mentionnées à l'article 12. Cet article reprend les dispositions de l'annexe I de la directive.

Le titulaire du certificat peut être une **personne physique ou morale**.

b) Les tiers de certification

L'avant-projet de loi prévoit que l'activité de certification puisse être exercée librement par une **personne physique ou une personne morale**. Il met en place un **système facultatif d'accréditation** des tiers de service de certification.

La plupart de ses articles ne s'appliquent qu'aux tiers de certification **accrédités par l'administration de la qualité et sécurité du ministère des Affaires économiques**, l'accréditation étant nécessaire pour la délivrance des certificats « qualifiés ».

Les conditions que les tiers de certification devront remplir pour obtenir et conserver l'accréditation sont inspirées directement de l'annexe II de la directive. Un texte réglementaire devra les préciser, ainsi que la procédure d'accréditation.

L'article 15 prévoit **la responsabilité des tiers de certification accrédités** pour tout préjudice subi par une personne qui s'est fiée au contenu d'un certificat « qualifié ». C'est donc le droit commun de la responsabilité qui s'applique aux tiers de certification qui délivrent des certificats ordinaires.

L'article 14 impose aux tiers de certification accrédités de conserver *« toutes les informations pertinentes concernant le certificat qualifié pendant une **durée de vingt ans**, en particulier pour pouvoir fournir une preuve de la certification en justice »*.

c) Le dispositif de création de la signature électronique

S'agissant des dispositifs sécurisés, l'avant-projet de loi reprend la formulation de l'annexe III de la directive.

De plus, il prévoit à l'article 20-1 que : *« Dès le moment de la création des données afférentes à la création de signature, le **titulaire du certificat est seul responsable de la confidentialité de ces données** »*.

LA SIGNATURE ELECTRONIQUE

DANEMARK

Immédiatement après l'adoption de la directive, le ministre de la Recherche a rendu public un avant-projet de loi sur les signatures électroniques (document n° 5), qui va faire l'objet d'une vaste consultation avant son dépôt au Parlement.

Comme le recommande la directive, cet avant-projet de loi traite de toutes les signatures électroniques, de quelque nature qu'elles soient. Son champ d'application diffère de celui de l'avant-projet de loi précédent, qui ne traitait que des signatures électroniques produites par un procédé de chiffrement asymétrique. Elaboré en 1998, ce texte avait été examiné par toutes les parties intéressées, mais le processus d'élaboration du projet avait été suspendu à cause de désaccords entre le ministère de la Justice et celui de la Recherche.

1) LA RECONNAISSANCE LÉGISLATIVE DE LA SIGNATURE ÉLECTRONIQUE

L'article premier de l'avant-projet sur les signatures électroniques détermine l'objet de la loi : promouvoir l'utilisation sûre et efficace des moyens électroniques de communication en fixant les exigences auxquelles doivent satisfaire, d'une part, les tiers de certification « qualifiés » pour l'utilisation des signatures électroniques, et, d'autre part, les systèmes sécurisés de création de signature électronique.

L'article 4 définit la signature électronique comme « *des données sous forme électronique, qui sont jointes ou liées logiquement à d'autres données électroniques grâce à un dispositif de création de signature et qui sont utilisées comme moyen d'authentification* ».

L'avant-projet reprend donc, à quelques mots près, la définition de la directive, mais n'établit pas de distinction entre « signature électronique » et « signature électronique avancée ».

2) LES EFFETS JURIDIQUES DE LA SIGNATURE ÉLECTRONIQUE

L'avant-projet de loi n'évoque pas explicitement les effets juridiques des signatures électroniques, car son objectif premier est de déterminer le régime juridique des tiers de certification qui délivrent des certificats « qualifiés », ainsi que définir les systèmes sécurisés de création de signature électronique.

Il ne remet pas non plus en cause le principe selon lequel les juges apprécient librement la valeur probante des éléments qui leur sont soumis.

Cependant, comme les tiers de certification qui exerceront leur activité dans le cadre de la loi garantiront la totale fiabilité des certificats, le respect des règles de création sécurisée des signatures électroniques devrait permettre aux tribunaux de reconnaître la valeur probante de ces dernières.

La question de la valeur juridique des signatures électroniques devrait être traitée de manière explicite ultérieurement. En effet, à la suite de la consultation qui avait été organisée au début de l'année 1998 sur l'avant-projet de loi précédent, lequel déterminait non seulement le régime juridique des tiers de certification, mais également la valeur juridique de certaines signatures électroniques, il était apparu que ce second aspect posait de nombreux problèmes transversaux et supposait la révision de plusieurs lois dans des domaines différents (droit des obligations, de la consommation...). C'est pourquoi le ministère de la Justice a institué une commission sur ce sujet, dans laquelle le ministère de la Recherche est représenté.

3) LES CONDITIONS DE VALIDITÉ DE LA SIGNATURE ÉLECTRONIQUE

La fiabilité de la signature électronique, dépend du respect de certaines conditions relatives :

- aux certificats ;
- aux tiers de certification ;
- au processus de création de la signature électronique.

a) Les certificats

L'avant-projet de loi définit les certificats d'une façon générale, mais ne traite que des certificats « qualifiés ». Cette appellation sera réservée aux certificats remplissant des conditions similaires, à quelques mots près, à celles qui figurent à l'annexe I de la directive.

Les certificats pourront être détenus par des personnes physiques ou par des personnes morales.

b) Les tiers de certification

L'avant-projet de loi consacre le principe du libre exercice de l'activité de certification par toute personne, physique ou morale, et oblige tous les tiers de certification à respecter la législation relative à la protection des données personnelles.

Pour le reste, l'avant-projet de loi ne traite que des tiers de certification qui délivreront des certificats « qualifiés ». Ces tiers de certification devront être accrédités par Telestyrelsen, qui est l'**Agence nationale des télécommunications**.

Telestyrelsen devra vérifier que les tiers de certification qui souhaitent délivrer des certificats « qualifiés » remplissent les conditions techniques, financières et humaines de sécurité et de fiabilité établies par l'avant-projet de loi et qui correspondent à celles de l'annexe II de la directive.

Ces tiers de certification auront l'interdiction de stocker ou de copier les éléments personnels qui permettent la création d'une signature électronique et dont ils auront pu avoir connaissance. Ils devront conserver pendant une période que l'avant-projet de loi qualifie de « raisonnable » tous les renseignements relatifs aux certificats.

L'avant-projet de loi prévoit également la **responsabilité** des tiers de certification qui délivrent des certificats « qualifiés » pour tout préjudice résultant du non-respect des règles qui leur seront imposées.

c) Le dispositif de création de la signature électronique

L'avant-projet de loi délègue au ministre de la Recherche le soin de prendre un règlement qui déterminera les conditions de la création sécurisée des signatures électroniques.

LA SIGNATURE ELECTRONIQUE

ESPAGNE

1) LA RECONNAISSANCE LÉGISLATIVE DE LA SIGNATURE ÉLECTRONIQUE

Le 21 octobre 1999, le Congrès des députés a ratifié le décret-loi sur la signature électronique, manifestant ainsi son approbation pour qu'il soit déposé comme **projet de loi** et examiné en urgence (document n° 6). Le texte est actuellement soumis à l'examen de la commission de la justice et de l'intérieur. Son adoption définitive devrait avoir lieu avant les prochaines élections législatives de mars 2000.

Dans son exposé des motifs, le projet de loi sur la signature électronique précise qu'il vise, « *dans le respect de la position commune relative à la directive sur la signature électronique, à établir une réglementation claire de son utilisation, en lui accordant pleine efficacité juridique et en prévoyant le régime applicable aux prestataires de service de certification* ».

A l'article 2, le projet définit la signature électronique et la signature électronique « avancée », en reprenant la même formulation que la directive.

2) LES EFFETS JURIDIQUES DE LA SIGNATURE ÉLECTRONIQUE

Le projet de loi reprend les dispositions de la directive. Il prévoit en effet :

- l'équivalence de la signature manuscrite et de la signature électronique « avancée », dans la mesure où elle se fonde sur un certificat qualifié et où elle a été créée par un dispositif sécurisé ;

- le non-rejet *a priori* de la valeur probante des autres signatures électroniques.

3) LES CONDITIONS DE VALIDITÉ DE LA SIGNATURE ÉLECTRONIQUE

La recevabilité comme moyen de preuve des signatures électroniques et la qualification de signature électronique « avancée » reposent sur des conditions relatives :

- aux certificats ;
- aux tiers de certification ;
- au processus de création de la signature électronique.

a) Les certificats

Ils ne pourront être détenus que par des **personnes physiques**, et leur validité sera limitée à **quatre ans**.

Le projet de loi définit seulement le contenu des certificats « reconnus », c'est-à-dire de ceux que la directive qualifie de « qualifiés ». Les certificats « reconnus » devront répondre aux mêmes critères que ceux posés à l'annexe I de la directive.

b) Les tiers de certification

L'activité de certification sera exercée par toute **personne physique ou morale**, sans que le projet de loi prévoie un quelconque système d'autorisation préalable.

Cependant, les tiers de certification devront se faire inscrire sur un registre spécifique, tenu par le ministère de la Justice. L'inscription ne sera réalisée qu'après la vérification de certaines conditions, particulièrement sévères pour les tiers qui délivreront des certificats « reconnus ». Ces derniers devront en effet remplir des conditions correspondantes à celles de l'annexe II de la directive.

Le projet de loi prévoit la **responsabilité** de tous les tiers de certification pour les préjudices résultant du non-respect des règles relatives à l'activité de certification. C'est pourquoi les tiers de certification qui délivrent des certificats « reconnus » devront disposer de ressources suffisantes pour pouvoir faire face à leur responsabilité. A cet effet, ils devront déposer **une garantie auprès d'un établissement financier**. Cette garantie sera limitée à **4 % du montant total des transactions susceptibles d'être réalisées grâce à leurs propres certificats**. Le projet de loi prévoit qu'un règlement pourra abaisser ce pourcentage à 2 %. En l'absence de plafonnement du montant des transactions pour lesquelles les certificats pourront être utilisés, la garantie devra être d'au moins un milliard de pesetas (c'est-à-dire environ 40 millions de francs).

Les tiers de certification auront l'obligation de garder pendant au moins quinze ans toutes les informations relatives aux certificats « reconnus ».

L'activité de tous les tiers de certification sera contrôlée par le Secrétariat général pour les communications, qui dépend du **ministère des Travaux publics**.

Le projet de loi prévoit aussi que le gouvernement pourra établir, par décret, des systèmes facultatifs d'accréditation.

c) Le dispositif de création de la signature électronique

Le projet de loi reprend les dispositions contenues à l'annexe III de la directive.

Les tiers de certification pourront faire certifier par des organismes d'évaluation *ad hoc* les dispositifs de création sécurisée de signature électronique.

LA SIGNATURE ELECTRONIQUE

ITALIE

1) LA RECONNAISSANCE LÉGISLATIVE DE LA SIGNATURE ÉLECTRONIQUE

L'article 15-2 de la loi n° 59 du 15 mars 1997 relative à la réforme de l'administration publique et à la simplification administrative (dite Loi Bassanini) affirme **la valeur juridique des documents électroniques**.

Il énonce en effet : « *Les actes, données et documents constitués par l'administration publique et par les personnes de droit privé à partir d'outils informatiques ou télématiques, les contrats rédigés sous cette même forme, ainsi que leur enregistrement ou leur transmission informatiques, sont valables et produisent tous les effets juridiques au regard de la loi. (...)* ».

Plus loin, le même alinéa prévoit que, dans le délai de six mois suivant l'entrée en vigueur de la loi, des dispositions réglementaires devront être prises pour déterminer les critères et les modalités d'application de ce principe.

Le décret n° 513 du 10 novembre 1997, relatif aux critères et aux modalités de constitution, d'archivage et de transmission des documents informatiques et télématiques (document n° 7), pris par le Président de la République pour l'application de la disposition légale susmentionnée définit la signature « digitale » comme « *le résultat de la procédure informatique fondée*

sur un système de clés asymétriques, une publique et une privée, qui permet au signataire, par l'intermédiaire de la clé privée, de garantir l'origine et l'intégrité d'un document informatique ou d'un ensemble de documents informatiques, et au destinataire, par l'intermédiaire de sa clé publique, de vérifier ces deux éléments ».

2) LES EFFETS JURIDIQUES DE LA SIGNATURE ÉLECTRONIQUE

Dans certaines conditions, définies par le décret n° 513 du 10 novembre 1997, **la signature « digitale » a la même valeur que la signature manuelle** et peut également remplacer un sceau, un poinçon, un tampon, ainsi que n'importe quel autre signe ou marque.

Ce texte prévoit que, tout comme la signature manuscrite, la signature « digitale » peut être **authentifiée par un officier ministériel** : celui-ci, après vérification de l'identité de l'intéressé et de la validité de la clé utilisée, atteste que la signature électronique a été apposée en sa présence par son titulaire.

En revanche, le décret ne traite pas du tout des autres signatures électroniques.

3) LES CONDITIONS DE VALIDITÉ DE LA SIGNATURE ÉLECTRONIQUE

Le décret pris par le Président du conseil des ministres le 8 février 1999 (document n° 8) détermine toutes les modalités techniques (définition des algorithmes utilisés pour produire et vérifier les signatures, caractéristiques des clés, obligations des détenteurs de clés et des tiers de certification, contenu des certificats...) permettant l'application du décret n° 513. Il précise ainsi les conditions d'équivalence entre la signature « digitale » et la signature manuelle, déjà définies par le décret n° 513 du 10 novembre 1997.

a) Les certificats

La signature « digitale » doit être produite par une clé privée dont la clé publique correspondante, préalablement certifiée par un prestataire de service de certification agréé, est encore valable. Les titulaires des certificats sont des **personnes physiques**. Le décret de 1999 précise toutes les informations nécessairement présentes sur les certificats. Ces exigences correspondent à celles de l'annexe I de la directive. **La validité de ces certificats ne peut excéder trois ans.**

b) Les tiers de certification

Les articles 8 et 9 du décret de 1997, qui précisent respectivement les critères que doivent remplir les tiers de certification et les obligations qu'ils doivent respecter, sont similaires aux exigences posées par l'annexe II de la directive. L'article 8 prévoit en particulier qu'il doit s'agir de **sociétés par actions dont le capital social est au moins égal à celui qui est exigé pour les établissements financiers.**

C'est l'**Autorité pour l'informatique dans l'administration publique**, organisme indépendant créé par un décret de février 1993 relatif aux systèmes informatiques publics, qui vérifie que les tiers de certification remplissent les conditions requises. Dans le secteur public, l'activité de certification est réalisée par les administrations elles-mêmes.

Le décret de 1997 ne comporte aucune disposition sur la responsabilité des tiers de certification, mais celui de 1999 leur impose le respect de mesures de sécurité et de dispositions techniques très sévères (établissement d'un plan général de sécurité dont la structure est définie par le décret lui-même ; enregistrement de toutes les opérations réalisées sur un journal de contrôle, qui doit être conservé pendant au moins dix ans ; obligation pour le personnel de remplir les différentes fonctions énumérées par le décret lui-même et de détenir certaines compétences...).

Les tiers de certification doivent conserver les clés publiques pendant au moins dix ans.

c) Le dispositif de création de la signature électronique

Les clés privées, produites par leur titulaire ou par les tiers de certification, ne doivent pas l'être à l'aide du système sur lequel elles seront utilisées ensuite. Le dispositif de création des clés privées doit remplir des exigences analogues à celle de l'annexe III de la directive.

Les tiers de certification n'ont pas le droit d'archiver les clés privées, qui doivent être conservées à l'intérieur d'un dispositif électronique *ad hoc*, les informations nécessaires à leur utilisation devant être stockées séparément.

LA SIGNATURE ELECTRONIQUE

LUXEMBOURG

1) LA RECONNAISSANCE LÉGISLATIVE DE LA SIGNATURE ÉLECTRONIQUE

Le projet de loi relatif au commerce électronique (document n° 9), adopté par le gouvernement le 10 mars 1999, traite des multiples aspects du commerce électronique. Son titre II, *De la preuve et de la signature électronique*, prévoit de reconnaître cette dernière.

Le gouvernement luxembourgeois envisage d'introduire une définition de la signature dans le chapitre du code civil relatif à la preuve littérale des obligations. En cela, il s'inspire des travaux menés par la France. En effet, le régime probatoire luxembourgeois est très proche du nôtre.

Le projet de loi prévoit d'insérer dans le **code civil un nouvel article 1322-1 définissant la signature par ses deux fonctions essentielles : l'identification du signataire et son adhésion au contenu de l'acte.**

Le même article précise que la signature pourrait être manuscrite ou électronique, et définit la signature électronique comme « *un ensemble de données liées de façon indissociable à l'acte, qui en garantit l'intégrité (...)* ».

Le projet de loi adopte donc une approche neutre sur le plan technologique. Toutes les technologies peuvent être employées, dès lors qu'elles permettent la réalisation des fonctions caractéristiques de la signature.

2) LES EFFETS JURIDIQUES DE LA SIGNATURE ÉLECTRONIQUE

Ils figurent dans la partie du projet de loi qui est consacrée aux autorités de certification. **Seules les signatures électroniques créées dans des conditions de sécurité optimales auront la même valeur que la signature manuscrite.** L'article 17 du projet de loi prévoit en effet qu'« *une signature électronique créée par un dispositif que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat agréé* » émis par un prestataire de service de certification accrédité bénéficie automatiquement des conséquences juridiques attachées à la signature au sens du code civil. Elle sera considérée comme équivalente à une signature manuscrite : elle sera recevable en justice et le juge ne pourra remettre en cause sa valeur probante intrinsèque.

En revanche, **la signature électronique qui ne satisfait pas à ces exigences ne bénéficiera pas de cette équivalence automatique**. En effet, si l'alinéa 2 de l'article 17 prévoit **qu'elle soit recevable en justice** (« *Une signature électronique ne peut être rejetée par un juge au seul motif qu'elle se présente sous forme électronique* »), la personne qui s'en prévaut devra convaincre le juge qu'elle répond à la définition fonctionnelle du code civil en apportant la **preuve de la fiabilité de la technique utilisée**. A défaut, l'acte auquel elle est attachée pourrait servir de commencement de preuve par écrit ou d'indice à l'appui d'une preuve par présomption.

* *

*

La loi du 22 décembre 1986 sur la preuve des actes juridiques reconnaît déjà aux enregistrements informatiques en matière civile la même force probante qu'aux écrits sous seing privé sous certaines conditions.

3) LES CONDITIONS DE VALIDITÉ DE LA SIGNATURE ÉLECTRONIQUE

Le projet de loi relatif au commerce électronique prévoit que les effets juridiques de la signature électronique dépendent de conditions relatives :

- aux certificats ;
- aux tiers de certification ;
- au processus de création de la signature électronique.

a) Les certificats

Le projet de loi envisage deux catégories de certificats : les certificats « agréés », qui correspondent aux certificats « qualifiés » au sens de la directive, et les autres certificats. La plupart des dispositions du projet ne concernent que les certificats « agréés ».

Qu'il soit « agréé » ou non, un certificat peut être détenu par **une personne physique ou morale**. Le projet de loi ne comporte aucune mention explicite sur la durée de validité des certificats.

Le contenu des certificats « agréés » sera déterminé par un règlement, qui devra correspondre à l'annexe II de la directive. Les certificats « agréés » devront en particulier comporter l'indication de leurs dates d'émission et d'expiration.

b) Les tiers de certification

Le projet de loi consacre le principe du **libre exercice de l'activité de certification par toute personne physique ou morale**. Il oblige les tiers de certification à tenir « *un registre des certificats disponibles au public, accessible en permanence par voie électronique* ».

Cependant, la délivrance des certificats « agréés » sera réservée aux tiers de certification accrédités, ainsi qu'à ceux qui ne sont pas accrédités, mais qui « *satisfont aux exigences de sécurité et de fiabilité déterminées par un règlement grand-ducal* ». Ce règlement devrait reprendre les termes de l'annexe II de la directive.

Les tiers de certification seront surveillés par l'**Autorité nationale d'accréditation et de surveillance**, qui sera également chargée de délivrer une accréditation à ceux d'entre eux qui en font la demande. **Le ministère de l'Economie devrait être désigné comme Autorité nationale d'accréditation et de surveillance**.

Le contenu de l'accréditation sera variable en fonction des critères de fiabilité du demandeur (garanties financières, techniques...) et du domaine dans lequel il souhaite exercer son activité.

Le projet de loi prévoit la **responsabilité de tous les tiers de certification**, qu'ils délivrent ou non des certificats « agréés », lorsque l'utilisation d'un certificat entraîne un dommage.

L'article 21 du projet de loi oblige les tiers de certification au « *secret concernant tous les renseignements qui leur sont confiés dans le cadre de leurs activités professionnelles*. » Le **secret professionnel** sera d'ordre public, et sa violation sera sanctionnée pénalement. Ces dispositions sont inspirées de la loi modifiée du 5 avril 1993 relative au secteur financier.

* *

*

Au début de l'année 1999, la Chambre de commerce luxembourgeoise s'est engagée dans un partenariat avec la société Globalsign pour délivrer des certificats numériques. Globalsign joue le rôle d'autorité de certification : elle émet des certificats numériques reposant sur la cryptographie à clé publique, les signe à l'aide de sa clé privée et en assure la gestion. La Chambre de commerce tient les fonctions de tiers certificateur en garantissant notamment la vérification des données relatives à l'établissement du certificat numérique.

c) Le dispositif de création de la signature électronique

Le projet de loi prévoit que le titulaire du certificat est « *responsable de la confidentialité et de l'intégrité du dispositif de création de signature qu'il utilise* ». Par ailleurs, il renvoie à un règlement grand-ducal qui précisera « *l'objet* ».

et le niveau de sécurité des dispositifs de création de signature ». Ce règlement transposera l'annexe III de la directive.

LA SIGNATURE ELECTRONIQUE

ROYAUME-UNI

1) LA RECONNAISSANCE LÉGISLATIVE DE LA SIGNATURE ÉLECTRONIQUE

Le 5 mars 1999, le ministère du Commerce et de l'Industrie a publié un document de consultation intitulé *Construire la confiance dans le commerce électronique*, dans lequel il indiquait comment il entendait **moderniser la législation, notamment pour permettre la reconnaissance de la signature électronique**. Une synthèse des réponses a été faite en juin 1999.

Le 23 juillet 1999, le gouvernement a publié l'**avant-projet de loi sur les moyens électroniques de communication** (document n° 10). Cet avant-projet se compose de quatre parties. La première traite de tous les prestataires des services dans le domaine de la cryptographie, parmi lesquels les tiers de certification. La seconde, qui est consacrée aux moyens de faciliter le commerce électronique, définit le régime juridique de la signature électronique.

L'avant-projet a été soumis à une consultation qui a pris fin le 8 octobre 1999. Le document de consultation de mars 1999 et l'avant-projet de loi ont donné lieu à deux rapports de la commission du commerce et de l'industrie de la Chambre des communes, publiés respectivement en mai et novembre 1999.

L'article 7 de l'avant-projet définit la signature électronique, lorsqu'elle est utilisée à des fins judiciaires, comme un bloc de données électroniques :

« a) qui est incorporé ou logiquement associé à un message électronique ; et

b) qui vise à être ainsi incorporé ou associé afin de servir à établir l'authenticité ou l'intégrité du message ou les deux ».

Le gouvernement estime qu'*« il ne serait pas sensé d'imposer une équivalence entre les moyens traditionnels de communication et les moyens électroniques d'un seul coup »*. Par conséquent, afin de permettre l'utilisation des nouvelles technologies de l'information et de la communication, il indique qu'il a choisi de se faire déléguer par la loi en préparation les pouvoirs de procéder de façon progressive à toutes les mises à jour, législatives ou réglementaires, nécessaires pour faciliter le développement du commerce électronique. Ainsi, des textes réglementaires pourront ultérieurement prévoir que les moyens électroniques de communication et d'archivage pourront remplacer les écrits, les communications postales, les signatures manuscrites, les sceaux, les témoignages.

D'après le discours du trône du 17 novembre 1999, qui présente le programme législatif du gouvernement, **le projet de loi sur les moyens électroniques de communication devrait être déposé au début de l'année 2000.**

2) LES EFFETS JURIDIQUES DE LA SIGNATURE ÉLECTRONIQUE

Dans son document de consultation, le gouvernement proposait l'instauration d'une présomption réfutable : la signature électronique, dans la mesure où elle aurait répondu à certains critères techniques et où elle aurait été confortée par un certificat délivré par un tiers de certification agréé, aurait identifié correctement le signataire et établi l'intégrité des données. Elle aurait donc été considérée comme équivalente à la signature manuscrite.

Ce point avait fait l'objet de vives critiques, notamment de la part de la commission parlementaire, car il renversait le système traditionnel de la charge de la preuve.

Dans son avant-projet de loi du 23 juillet 1999, le gouvernement a abandonné cette proposition. L'article 7 indique que *« dans tout procès, une signature électronique incorporée ou logiquement associée à un message électronique donné, ainsi que la certification d'une telle signature, sont toutes les deux recevables comme preuves de tout élément relatif à l'authenticité ou à l'intégrité du message »*.

Le même article précise qu'une signature est considérée comme certifiée si quelqu'un -avant ou après la transmission du message- a établi que la signature ou le procédé de création de la signature sont des moyens valables d'établir l'authenticité et/ou l'intégrité du message.

La loi laisserait donc aux tribunaux le soin d'apprécier la valeur d'une signature électronique, mais le gouvernement a l'intention de clarifier ce point ultérieurement.

Certains commentateurs s'interrogent sur l'utilité de cet article 7, puisque **la recevabilité des signatures électroniques est déjà reconnue par la jurisprudence.**

3) LES CONDITIONS DE VALIDITÉ DE LA SIGNATURE ÉLECTRONIQUE

La recevabilité en justice de la signature électronique est liée au respect de conditions relatives :

- aux certificats ;
- aux tiers de certification ;

- au processus de création de la signature électronique.

a) Les certificats

L'avant-projet de loi de juillet 1999 mentionne les certificats sans autre précision. Ce point devrait être précisé lors de la mise en place du système d'accréditation des tiers de certification.

b) Les tiers de certification

L'avant-projet de loi du 23 juillet 1999, dans son article premier, oblige le secrétaire d'Etat au Commerce et à l'Industrie à tenir un registre de tous les prestataires des différents services liés à l'utilisation de la cryptographie. Cette obligation vaut en particulier pour les tiers de certification accrédités. L'article 2 impose au ministre de veiller à ce que des dispositions relatives à l'octroi de l'agrément, au règlement des litiges, à la modification et au retrait de l'agrément, et établissant certains principes, comme ceux de la **libre accréditation** et de la **variabilité du contenu de l'accréditation soient prises**. Le secrétaire d'Etat pourrait toutefois confier cette mission à un tiers.

Ainsi, le gouvernement a abandonné l'idée, développée dans son document de mars 1999, de mettre en place un système d'accréditation par voie réglementaire. En ceci, il a suivi la recommandation de la commission parlementaire, qui lui conseillait de s'en remettre à l'**autorégulation des milieux industriels** et de n'intervenir qu'en cas d'échec. Le gouvernement a donc décidé de faire confiance à un consortium industriel, *l'Alliance pour le commerce électronique*. Celui-ci devrait établir, en relation avec le ministère du Commerce et de l'Industrie, un schéma d'accréditation avant la fin de l'an 2000.

Le gouvernement a également décidé de ne pas prendre de dispositions sur la responsabilité des tiers de certification, mais il attend de ces derniers qu'ils expliquent clairement à leurs clients l'étendue et les limites de leurs responsabilités.

Par ailleurs, en mars 1999, le gouvernement a annoncé qu'il renonçait à la proposition que les tiers de certification fussent accrédités à la seule condition d'avoir mis en place un **système obligeant le signataire à confier sa clé privée à un tiers pour la fournir à la police sous certaines conditions**, notamment lors d'enquêtes criminelles. En effet, ce point avait été vivement contesté par les industriels, les groupes de défense des libertés publiques et les experts en informatique. La commission parlementaire avait également critiqué ces dispositions. Dans son rapport de novembre 1999, elle met d'ailleurs en garde le gouvernement contre toute tentative de rétablissement du système. Elle indique qu'elle restera vigilante à ce sujet lors du dépôt du projet de loi.

c) Le dispositif de création de signature électronique

Il ne figure pas dans l'avant-projet de loi. Il devrait être mis en place par voie de consensus dans les milieux industriels.

ANNEXE 5

LISTE DES PERSONNES ENTENDUES

Votre commission des Lois a procédé à l'audition de **Mme Isabelle Falque-Pierrotin**, maître des requêtes au Conseil d'Etat, rapporteur général du groupe d'étude du Conseil d'Etat, auteur du rapport « Internet et les réseaux numériques ».

Elle a pu prendre la mesure des aspects techniques du présent projet de loi lors de l'audition, appuyée sur une démonstration sur matériel informatique, de représentants de la **société IBM** : Mme Muriel Collignon, responsable des offres de sécurité, M. Jean-François Ragu, architecte sécurité des réseaux et responsable de la cellule « tests d'intrusion », M. Bernard Naudin, responsable des offres « e-business », et M. Gilles Ragueneau, directeur des relations extérieures.

Votre rapporteur tient à remercier le **service de l'informatique et des technologies nouvelles du Sénat** pour les explications fournies sur le cryptage et la signature électronique.

Outre les commissaires du Gouvernement, le rapporteur a reçu en audition les représentants :

- du Conseil supérieur du notariat ;
- de l'Association française des entreprises privées ;
- de l'Association des professionnels de la gestion électronique de documents (APROGED) ;
- de l'Association des greffiers de commerce de France ;
- de la Chambre nationale des huissiers de justice ;
- de l'Association française des banques ;
- de la société Vivendi.

Il a de plus entendu :

- M. Jérôme Huet, professeur d'université.