Document mis en distribution le 28 février 2000

N° 2197

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

ONZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 23 février 2000.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE (1) SUR LE PROJET DE LOI, ADOPTÉ PAR LE SÉNAT, *portant adaptation du* **droit de la preuve** *aux technologies de l'information et relatif à la* **signature électronique,**

PAR M. CHRISTIAN PAUL,

Député.

(1) La composition de cette commission figure au verso de la présente page.

Voir les numéros :

Sénat : **488** (1998-1999)**, 203** et T.A. **70** (1999-2000).

Assemblée nationale : **2158**.

Droit civil.

La commission des Lois constitutionnelles, de la législation et de l'administration générale de la République est composée de : Mme Catherine Tasca, *présidente* ; MM. Pierre Albertini, Gérard Gouzes, Mme Christine Lazerges, *vice-présidents* ; MM. Richard Cazenave, André Gerin, Arnaud Montebourg, *secrétaires* ; MM. Léo Andy, Léon Bertrand, Emile Blessig, Jean-Louis Borloo, Patrick Braouezec, Mme Frédérique Bredin, MM. Jacques Brunhes, Michel Buillard, Dominique Bussereau, Christophe Caresche, Patrice Carvalho, Jean-Yves Caullet, Mme Nicole Catala, MM. Olivier de Chazeaux, Pascal Clément, Jean Codognès, François Colcombet, François Cuillandre, Henri Cuq, Jacky Darne, Camille Darsières, Jean-Claude Decagny, Bernard Derosier, Franck Dhersin, Marc Dolez, Renaud Donnedieu de Vabres, René Dosière, Renaud Dutreil, Jean Espilondo, Mme Nicole Feidt, MM. Jacques Floch, Raymond Forni, Roger Franzoni, Pierre Frogier, Claude Goasguen, Louis Guédon, Guy Hascoët, Philippe Houillon, Michel Hunault, Henry Jean-Baptiste, Jérôme Lambert, Mme Claudine Ledoux, MM. Jean-Antoine Léonetti, Bruno Le Roux, Mme Raymonde Le Texier, MM. Jacques Limouzy, Thierry Mariani, Louis Mermaz, Jean-Pierre Michel, Ernest Moutoussamy, Mme Véronique Neiertz, MM. Robert Pandraud, Christian Paul, Vincent Peillon, Dominique Perben, Henri Plagnol, Didier Quentin, Bernard Roman, Jean-Pierre Soisson, Frantz Taittinger, Jean Tiberi, Alain Tourret, André Vallini, Alain Vidalies, Jean-Luc Warsmann.

SOMMAIRE

—

Pages

MESDAMES, MESSIEURS,

La croissance du commerce électronique, dont le dynamisme quotidien ne laisse pas d'étonner, fascine autant qu'elle inquiète. Les données transmises resteront-elles confidentielles ? Comment s'assurer du consentement et de l'identité du cocontractant ? Quelle est la valeur du document informatique ? Telles sont, entre autres, les nombreuses interrogations que se posent les acteurs de la nouvelle économie de l'Internet. Conscient des enjeux en termes de concurrence internationale, de croissance et donc d'emploi, les pouvoirs publics ne pouvaient rester immobiles face à ces défis juridiques et techniques.

Lors des premières rencontres parlementaires sur la société de l'information, organisées à l'Assemblée nationale le 5 octobre 1999, dont le thème était « Internet : la révolution numérique crée-t-elle la révolution juridique ? », Mme Elisabeth Guigou déclarait : *« La sécurisation et l'adaptation des règles de la transaction électronique conditionnent le développement du commerce sur la toile. Sans sécurité des échanges, le commerce électronique ne pourra pas prendre un essor significatif. Il est magnifique de pouvoir commander des fleurs sur Internet, de les choisir, de les payer avec un numéro de carte bancaire et de les expédier à l'élu(e) de son cœur. Mais il serait aussi rassurant de savoir que personne ne pourra s'approprier ce même numéro pour vider totalement votre compte en banque, en commandant un billet d'avion pour fuir aux Tuamotu. »*

Ce projet de loi constitue la première réponse législative apportée au besoin de sécurité ainsi illustré par la garde des sceaux. Il y a désormais une réelle urgence à ce que d'autres mesures de confiance soient prises par notre pays, singulièrement dans le domaine de la protection des données personnelles et de la cryptologie.

Alors que l'essor durable du commerce électronique requiert une sécurité juridique accrue pour ses acteurs (I), le projet de loi relatif à la preuve et à la signature électronique s'inscrit dans une stratégie globale d'entrée dans la société de l'information (II). Il inaugure une adaptation de notre droit à la révolution numérique, en introduisant une innovation fondamentale dans le code civil (III).

I. — L'ESSOR DURABLE DU COMMERCE ELECTRONIQUE REQUIERT UNE SECURITE JURIDIQUE ACCRUE POUR SES ACTEURS.

La croissance des transactions électroniques entraînera nécessairement celle des actes juridiques recourant aux procédés de signature électronique et rend donc nécessaire l'admission de l'écrit électronique en preuve (A). Par ailleurs, le commerce électronique doit offrir une sécurité juridique aux entreprises comme aux consommateurs (B).

A. LA CROISSANCE DES TRANSACTIONS ÉLECTRONIQUES ENTRAINERA NECESSAIREMENT CELLE DES ACTES JURIDIQUES RECOURANT AUX PROCEDES DE SIGNATURE ELECTRONIQUE ET REND DONC NECESSAIRE L'ADMISSION DE L'ECRIT ELECTRONIQUE EN PREUVE.

En termes de volume, le commerce électronique en France demeure d'importance modeste puisque le chiffre d'affaires des sites français marchands serait, d'après le Benchmark group, de 1,3 milliard de francs en 1999, tandis que celui réalisé par le minitel atteindrait 8 milliards de francs. Afin d'affiner l'analyse de ces grands agrégats, il conviendrait de définir les industries composant le secteur des technologies de l'information ; or la composition sectorielle de l'INSEE n'isole pas un tel secteur. Cette imperfection statistique explique nombre des divergences d'estimations rencontrées en la matière. Ainsi, selon l'institut IDC le poids du commerce électronique dans le monde atteindrait 68 milliards de dollars en 1999 alors que le groupe *eMarketer* l'estime pour la même période à 98,4 milliards de dollars. Si l'on se fie à ces organismes, le commerce électronique devrait avoisiner les 1 000 à 1 200 milliards de dollars en 2003. Néanmoins, un certain accord semble exister pour estimer que le secteur des « technologies de l'information » représenterait 5 % du PIB français contre 15 % aux Etats Unis.

Cependant, le dynamisme de l'e-économie s'apprécie davantage ***en termes de flux*** et cela quel que soit le segment d'analyse retenu. Du point de vue financier, au premier semestre 1999 quelques 129 *starts up* françaises contre 111 en 1998 ont été financées à hauteur de 872 millions de francs contre 675 millions l'année précédente. En outre, d'après le journal du net (www.journaldunet.com), le début de l'année 2000 devrait être marqué par l'accession de vingt-quatre entreprises de ce secteur au nouveau marché.

Le marché de l'emploi n'échappe pas à cette tendance ; preuve en est le nombre de CV disponibles sur le Web qui a été multiplié par 200 entre 1994 et 1999 pour atteindre 4 900 000 dans le monde. Selon une étude

menée par *Computer Economics*. Là encore, le développement probable des procédures de recrutement électronique rendra nécessaire une protection juridique accrue pour les contractants, à laquelle la fiabilité de la signature électronique participe pleinement. Les Etats-Unis font figure de précurseurs puisque 55 % des diplômés américains auraient envoyé leur CV à un service d'emploi en ligne en 1999.

D'un point de vue ***macro-économique*** et si l'on se réfère encore aux Etats-Unis, l'emploi dans le secteur des nouvelles technologies devrait croître à un rythme double de celui des autres secteurs, les salaires y étant 40 % supérieurs à ceux que l'on constate en moyenne dans l'industrie. Une dynamique comparable, bien que de moindre ampleur, semble à l'œuvre en France où, selon le cabinet *Markess international* cité par la Mission sur le commerce électronique, 250 petites entreprises auraient été créées en France en 1998 autour des technologies d'Internet, employant 12 000 personnes.

En ce qui concerne l'impact de la croissance de ce secteur sur le niveau des prix, l'étude menée par le cabinet allemand *Stifung Warentest* à la demande de la Commission européenne (www.euro.ucl.ac.be) conclut à un niveau de prix sur Internet inférieur de 15 % à ceux pratiqués par les distributeurs traditionnels. Toutefois, on ne peut conclure définitivement à un effet désinflationniste du commerce électronique, ne serait-ce qu'en raison de l'apparition de nouveaux intermédiaires qui peuvent compenser l'effet-prix observé dans certaines secteurs : par exemple, les activités de marketing, l'émergence de sites de référencement, ou la création de bouquets thématiques filtrant l'accès à des sites préalablement choisis.

Par ailleurs, les perspectives de croissance actuelles devraient conduire à une hausse de ***l'équipement informatique des ménages***. D'un point de vue micro-économique, l'équipement en ordinateur semble s'apparenter à un bien dit « supérieur », à savoir un bien dont la croissance est plus que proportionnelle à celle du revenu. Ainsi, en 1998 la demande finale des ménages pour ce secteur a connu un véritable rebond, près de 35 % de la croissance de leur consommation s'expliquant en 1998 par les postes « télécommunications » et « appareils électroniques ». En conséquence, le nombre d'internautes serait passé en France de 3,7 millions de personnes en 1998 à 5,21 en 1999.

Cette croissance du nombre des utilisateurs de la Toile ne pourra rester sans effets sur le commerce électronique et impose de définir sans tarder un cadre juridique sécurisant pour les utilisateurs. Toutefois, force est de constater que le taux d'équipement des ménages en ordinateurs (19 % selon l'INSEE) demeure toujours inférieur à celui de nos principaux partenaires (27 % en Europe et 35 % en Allemagne).

B. LE COMMERCE ELECTRONIQUE DOIT OFFRIR UNE SECURITE JURIDIQUE AUX ENTREPRISES COMME AUX CONSOMMATEURS.

Le rapport présenté par M. Francis Lorentz au nom de la Mission sur le commerce électronique (*cf.* www.finances.gouv.fr) définit le commerce électronique comme l'ensemble des échanges électroniques liés aux activités commerciales : flux d'information et transactions concernant des produits ou des services. Ainsi appréhendé, il s'étend aux relations entre les entreprises, entre les entreprises et les administrations, entre les entreprises et les particuliers et prend appui sur toutes les formes de numérisation possibles : Internet, minitel, téléphone, télévision...Toutefois, il est également convenu de distinguer dans le commerce électronique, celui qui se développe exclusivement entre les entreprises (dit *B to B* ou *business to business*) de celui qui met en relation une entreprise et un particulier (*B to C* ou *business to consumer*).

Le phénomène de commerce électronique n'est pas nouveau puisque les entreprises l'ont développé depuis une dizaine d'année sous la forme dite d'« EDI » (échange de données informatisées). Les réseaux EDI permettent de transmettre électroniquement des documents standardisés, tels que factures, commandes ou bordereaux de livraison. Il convient de noter qu'en France les échanges sur EDI utilisent encore rarement le réseau Internet et représentent 800 milliards de francs.

A cet égard, les entreprises françaises ont fait un effort significatif en matière de connexion à Internet : en janvier 1999, 405 des 1 500 premières entreprises françaises (27 %) avaient ouvert un site web français et 7 % un site international. Cependant 13 % seulement de ces entreprises faisaient du commerce électronique. En ce qui concerne les PME-PMI, une récente étude menée par UFB-Locabail (www.ufb-locabail.fr) a établi que 61% d'entre elles étaient connectées à Internet contre 72 % de leurs homologues du G4. Néanmoins, le retard relatif des entreprises françaises devrait se combler progressivement si la croissance de leur taux de connexion (+ 21 % entre 1998 et 1999) se prolonge encore quelques années et si elles acquièrent la certitude que le commerce électronique leur procure la même sécurité juridique que le commerce traditionnel.

Quant au commerce résidentiel *(B to C)* ne représenterait que 20 % du volume des échanges sur Internet, les 80 % restants étant le fait des entreprises. Au total, on constate donc que les cyberconsommateurs sont encore peu nombreux, 10 % des internautes français en 1999 contre 4 % en 1996 selon une étude du *Benchmark Group*. Or, un des obstacles au développement du commerce électronique des particuliers tient à l'incertitude juridique ressentie par les consommateurs. En effet, la

spécificité du e-commerce tient au fait qu'il s'agit d'un échange qui se développe en l'absence des parties puisque le commerçant ne connaît pas son client qui ne le connaît pas davantage. C'est pourquoi il est essentiel de pouvoir identifier son partenaire dans une relation commerciale ; c'est à cette exigence que devraient répondre les procédés de signatures électroniques cryptées.

D'après l'étude allemande financée par la Commission européenne citée plus haut, l'attitude réservée des consommateurs allemands et européens tient avant tout aux inquiétudes sur la sécurité du paiement en ligne mais aussi au manque de clarté de la situation juridique du consommateur et du fournisseur. Là encore, le dispositif du projet de loi, en mettant en place les conditions d'une confidentialité et d'une sécurisation accrues pour les conventions conclues en ligne, grâce à la signature électronique et à l'admission en preuve des documents numériques, devrait favoriser un développement durable de cette activité et de tous les systèmes de vente par correspondance.

Auditionnée par votre rapporteur, l'*Union fédérale des consommateurs* (UFC) a néanmoins fait part de sa préoccupation quant au développement du commerce en ligne et a regretté qu'il soit envisagé d'accorder à l'écrit numérique une valeur probante identique à celle de l'écrit sur papier. Sa représentante a exprimé sa préférence pour un système s'inspirant de celui adopté au Québec, qui donne à l'écrit électronique une valeur probante inférieure à celle de l'écrit sur papier.

Pour autant, force est de constater que le projet de loi ne modifie en rien les règles d'ordre public applicables au droit de la consommation qui sont particulièrement protectrices pour les consommateurs. En outre, le projet de loi apporte un double progrès pour leur protection, d'une part, en rendant l'écrit électronique admissible en tant que preuve devant le juge et, d'autre part, en lui conférant une valeur probante identique à celle du document sous seing privé, ce qui ne peut que préserver les intérêts des personnes ayant commandé en ligne.

Il faut ajouter que, sous réserve que soit sécurisée la signature électronique selon des modalités qui relèvent du décret, le texte du projet de loi améliore la sécurité des transactions en ligne, ce qui ne peut être que bénéfique aux consommateurs. Enfin, l'émergence prochaine d'autorités de certification, prévues par l'article 3 du projet de loi qui renvoie les modalités d'exécution à un décret en Conseil d'Etat, devrait considérablement améliorer la fiabilité juridique du commerce électronique. Interrogées par votre rapporteur, les entreprises présentes dans le secteur de la certification ont indiqué que le coût d'un certificat pour un particulier

devrait être modique, de l'ordre de quelques dizaines de francs, et pourrait rapidement décroître dans les prochaines années en raison de l'amortissement rapide des investissements réalisés.

Si les particuliers expriment sans conteste une demande de sécurité juridique, il en est de même pour les professionnels. Entendue par votre rapporteur, la *Chambre de commerce et d'industrie de Paris* a ainsi fait part de la demande des entreprises d'une clarification de la valeur de la signature électronique et de sa force probante, incertaine à l'heure actuelle.

Enfin, il convient de souligner que l'augmentation du commerce électronique s'accompagnera inévitablement ***d'une croissance du contentieux***. A l'heure actuelle, l'essentiel des contentieux paraît se concentrer sur les questions de paiement en ligne ; mais ces difficultés pourraient être réduites par les procédés fiables de signature électronique. En revanche, selon des observations américaines (www.salon.com), certaines grandes sociétés américaines sont aussi l'objet de poursuites pour non-respect des délais de livraison des produits commandés en ligne. Il est probable que les mêmes phénomènes vont être observés en France, ce qui rend d'autant plus utile une législation clarifiant pour les acteurs et pour le juge chargé de trancher les différends, les règles permettant l'authentification de la signature électronique, tout en définissant la valeur probante du document électronique.

II. — LE PROJET DE LOI RELATIF A LA PREUVE ET A LA SIGNATURE ELECTRONIQUES S'INSCRIT DANS UNE STRATEGIE GLOBALE D'ENTREE DANS LA SOCIETE DE L'INFORMATION.

Sans entrer dans le détail de toutes les mesures prises par les pouvoirs publics et les organisations internationales en matière d'adaptation du droit et des procédures au développement d'Internet, force est de constater que celles-ci abordent de façon globale les exigences de la société de l'information et que le contexte est favorable à l'intervention du législateur pour sécuriser les relations juridiques sur Internet.

Le programme du Gouvernement pour la société de l'information (PAGSI) se veut une réponse d'ensemble, progressive et adaptée aux enjeux de la société de l'information (A). Cette préoccupation est partagée au plan international (B).

A. LE PROGRAMME DU GOUVERNEMENT POUR LA SOCIETE DE L'INFORMATION SE VEUT UNE REPONSE D'ENSEMBLE, PRO-

GRESSIVE ET ADAPTEE AUX ENJEUX DE LA SOCIETE DE L'INFORMATION.

Présenté le 18 janvier 1998, le programme d'action gouvernemental pour la société de l'information (PAGSI) tend à créer une mobilisation de l'ensemble des acteurs pour favoriser le développement des nouvelles technologies de l'information. En effet, comme l'a déclaré Lionel Jospin le 26 août 1999 à Hourtin, lors de l'université de la communication, *« l'impulsion ainsi donnée par le Gouvernement était indispensable. L'attentisme n'était plus de mise. S'en remettre à la seule spontanéité du marché – en l'occurrence prise en défaut – aurait été dangereux. Il était de la responsabilité de l'Etat de donner le signal d'un vaste mouvement collectif ».* Ainsi, d'après le SJTIC, qui a en charge le suivi de l'exécution de ce programme, 153 des 218 objectifs fixés sont atteints soit un taux de réalisation en deux ans de 70 % www.premier-ministre.gouv.fr. En réponse à la question d'un député, le Gouvernement a indiqué que ce plan repose tant sur des moyens budgétaires ainsi que sur des adaptations réglementaires et législatives (JO AN du 22 juin 1998, p. 3403, www.journal-officiel.gouv.fr).

En matière budgétaire d'abord, les crédits consacrés à la mise en œuvre du PAGSI se sont élevés, d'après la direction du Budget, à 5,76 milliards de francs sur deux ans, dont 3,6 milliards en 1999. En ce qui concerne les seuls crédits informatiques, ils se sont élevés à 660 millions de francs en 1998 et correspondent aux actions informatiques de modernisation de l'Etat, qui incluent notamment la mise en ligne de serveurs et de données sur Internet ou le développement de téléprocédures.

D'ores et déjà, il existe plusieurs sites publics sur lesquels l'internaute se voir proposer des services de commande par Internet, sans paiement direct en ligne. Il en est ainsi du site de la documentation française (www.ladocfrancaise.gouv.fr) ou l'internaute peut remplir et envoyer un bon de commande en ligne, le paiement lui-même s'effectuant par les voies traditionnelles. Notre assemblée n'est pas en reste et mène actuellement une étude sur la réalisation d'un service de paiement en ligne des documents parlementaires, qui pourrait aboutir dans le courant de l'année 2000. Par ailleurs, l'unique site public qui propose un paiement sécurisé par carte bancaire est celui de la Monnaie de Paris.

En outre, l'information administrative proposée sur Internet au public se développe et déjà plus de 80 % des formulaires les plus utilisés sont disponibles en ligne. En application d'une circulaire du Premier ministre du 31 décembre 1999 (JO du 7 janvier 2000, www.journal-officiel.gouv.fr), les ministères devront avoir procédé à la mise en ligne de

la totalité de leurs formulaires d'ici l'été prochain. Cette circulaire est accompagnée d'une charte de mise en ligne qui précise les droits et les obligations des services publics concernés.

En ce qui concerne les particuliers, les formulaires déclaratifs relatifs à l'impôt sur le revenu (n° 2042) seront mis en ligne à partir du 21 février 2000. Sous réserve de l'accord de la CNIL, le formulaire, après avoir été rempli en ligne, téléchargé sur le disque dur du contribuable, pourra être envoyé en fichier attaché, au centre informatique des Impôts. L'identité du contribuable sera authentifiée grâce à son code (FIP) qu'il sera invité à préciser. Pour les entreprises, le ministère de l'économie et des finances prévoit que deux téléprocédures totalement dématérialisées seront proposées au début de l'année 2000 : la télédéclaration et le paiement de la TVA ainsi que la télédéclaration d'échanges de biens (*cf.* réponse parue au JO *Questions* AN du 2 août 1999, p. 4679, www.journal-officiel.gouv.fr). Il est indiscutable que le développement de la signature électronique, accompagné d'un renforcement de sa qualité juridique, modifiera les relations entre les administrés et l'administration et contribuera à les simplifier tout en renforçant l'efficacité du service public.

Dans le domaine législatif, il convient de rappeler que l'article 4 de la loi du 11 février 1994 relative à l'initiative et à l'entreprise individuelle admettait la transmission d'une déclaration administrative par la voie électronique. La loi dispose qu'un document électronique répondant aux exigences posées « [tient] *lieu d'une déclaration écrite ayant le même objet* ». Au-delà de ces premiers pas législatifs, deux mesures récentes tendent, également, à favoriser la croissance de l'économie de la société de l'information.

D'une part, la recherche d'un effet de levier sur le financement privé en faveur de l'innovation s'est traduite par des dispositions fiscales favorables dans les lois de finances pour 1998 et 1999. Ainsi, un régime fiscal incitatif a été élaboré en faveur des bons de souscriptions de parts attribués par des jeunes entreprises à certains de leurs salariés. Ce dispositif, réservé initialement aux entreprises de moins de sept ans, a été étendu aux entreprises de moins de quinze ans par la loi de finances pour 1999. L'émission de ces bons est un moyen pour les entreprises innovantes d'attirer des collaborateurs de haut niveau auxquels elles ne sont pas en mesure d'offrir une rémunération comparable à celle à laquelle ils pourraient prétendre dans les entreprises plus importantes. D'autre part, l'adoption en juillet 1999 de la loi sur l'innovation et la recherche tend à favoriser la mobilité des chercheurs et des enseignants en leur offrant la possibilité de participer à la création d'une entreprise, de faire de la consultance ou encore de siéger dans les conseils d'administration.

B. UNE PREOCCUPATION PARTAGEE PAR LES ORGANISATIONS INTERNATIONALES

Deux instances internationales se sont intéressées tout particulièrement aux questions de la signature électronique : la Commission des Nations-Unies pour le droit commercial international (CNUDCI), puis l'Union européenne.

1. La CNUDCI tente d'élaborer un projet de règles uniformes sur les signatures électroniques

Alors que se tient à New York, du 14 au 25 février 2000, la 36e session du groupe de travail sur le commerce électronique, le dernier état de la question, publié le 9 décembre 1999, montre que le projet de règles uniformes sur les signatures électroniques s'oriente vers la définition d'un cadre neutre quant aux technologies employées, démarche également retenue par le Gouvernement français. En effet, l'article 3 du projet de loi dispose que la signature, qu'elle soit électronique ou non, *« identifie celui qui l'appose et manifeste son consentement aux obligations qui déroulent de cet acte »* ; il est, en outre, précisé que *« 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 CNUDCI (www.uncitral.org) souhaite prévenir une discordance entre les règles juridiques applicables au commerce électronique, en « *offrant un ensemble de normes sur lesquelles se fonder pour reconnaître les effets juridiques des signatures numériques, avec l'aide éventuelle des autorités de certification pour lesquelles un certain nombre de règles de base sont aussi prévues* ». Dans l'état actuel de la rédaction de l'article 2 du projet de la CNUDCI, la définition de la signature électronique proposée est la suivante : « *des données sous forme électronique contenues dans un message de données ou logiquement associées audit message et pouvant être utilisées pour identifier le détenteur de la signature dans le cadre de messages de données et indiquer qu'il approuve l'information qui y est contenue* ». Tout en étant plus lourde que celle retenue dans le présent projet de loi, la définition de la signature électronique proposée par la CNUDCI insiste également sur sa double fonction : identification de la personne et manifestation de son consentement.

En outre, à la différence de la France, la CNUDCI retient la distinction entre signature électronique simple et « signature électronique renforcée ». Celle-ci désigne une signature dont on peut démontrer, par l'application d'une procédure de sécurité, *« qu'elle est particulière au détenteur de la signature aux fins pour lesquelles elle est utilisée, qu'elle a*

été créée et apposée au message de données par le détenteur de la signature ou à l'aide d'un moyen dont seul le détenteur a le contrôle, qu'elle a été créée et est liée au message de données auquel elle se rapporte d'une manière qui offre une garantie fiable quant à l'intégrité du message ». Si le Gouvernement a fait le choix, dans la rédaction retenue pour les articles 1616-1 et 1322-2 du code civil, d'un type unique de signature, celle-ci se rapproche de ce que la CNUDCI qualifie de signature renforcée.

Par ailleurs, l'article 11 du projet de la CNUDCI, relatif à la foi accordée aux signatures électroniques, dispose dans son premier alinéa qu'une personne est fondée à ne pas se fier à une signature électronique dans la mesure où « *il n'est pas raisonnable de le faire* ». La rédaction de ce considérant de principe peut paraître curieuse car il pourrait en résulter une présomption de non-fiabilité de la signature numérique, la référence au caractère raisonnable laissant ouverte une possibilité de contestation. En fait, il semble plutôt que la CNUDCI souhaite proportionner le degré d'exigence de fiabilité d'une signature au montant et à l'importance de la transaction à laquelle elle se rattache. La solution retenue par le Gouvernement constitue un cadre juridique plus rigoureux qui s'impose quel que soit le montant de la transaction effectuée. Le texte initial dispose en effet que la signature électronique bénéficie d'une présomption de fiabilité et est admissible en tant que 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 »* (article 1316-1 du code civil).

En revanche, le texte de la CNUDCI aborde la question de la reconnaissance mutuelle internationale des signatures, ce que ne fait pas explicitement le projet de loi. En effet, l'article 13 du texte onusien pose le principe de la non-discrimination entre les signatures électroniques dans les termes suivants : *« Pour déterminer si un certificat* [ou une signature électronique] *produit légalement ses effets, il n'est pas tenu compte du lieu ou le certificat* [ou la signature électronique] *a été émis, ni de l'État dans lequel l'émetteur a son établissement. Les certificats émis par un prestataire de service de certification sont reconnus comme équivalent juridiquement aux certificats émis par les prestataires de services de certification soumis* [à la loi de l'état adoptant] *si les pratiques du prestataire de services de certification étrangers offrent un niveau de fiabilité au moins équivalent à celui requis en vertu de* [la loi de l'état adoptant]. *Cette reconnaissance peut se faire par une décision publiée par l'état ou par un accord bilatéral ou multilatéral entre les états concernés. »* Le droit applicable sera donc celui des contrats, le texte du projet de loi renvoyant au juge le soin de trancher les conflits de preuve (article 1316-2 du code civil) en cas d'absence de conventions sur la preuve (droit supplétif).

2. La directive européenne du 13 décembre 1999 offre un cadre juridique favorable au développement de la signature électronique et du commerce en ligne.

Comme l'a souligné M. Francis Lorentz devant votre rapporteur, l'un des enjeux majeurs de la compétition actuelle réside dans la constitution d'un espace de droit dans lequel le fournisseur et le consommateur se sentent en confiance. La création d'un tel espace semble bien engagée en Europe ce qui pourrait lui conférer un avantage concurrentiel certain vis-à-vis des Etats-Unis qui rencontrent des difficultés juridiques en raison de la variété des droits des Etats fédérés et d'une résistance à l'intervention unificatrice de l'Etat fédéral.

Le projet de loi relatif à la signature électronique n'est pas à proprement parler une transposition de la directive 1999/93/CE du 13 décembre 1999, car sa présentation en Conseil des ministres, au début du mois de septembre 1999, est intervenue avant la conclusion des travaux communautaires. Le projet de loi est cependant en conformité avec le dispositif communautaire, qui sera totalement transposé dans notre droit interne une fois les décrets d'application du projet adoptés.

Après avoir défini la signature électronique comme *« une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification »*, l'article 2 de la directive précise ce qu'elle entend par « signature électronique avancée ». Il s'agit d'une signature qui respecte les exigences suivantes : *« a) être liée uniquement au prestataire, b) permettre d'identifier le signataire, c) être créée par des moyens que son 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 »*.

La question se pose de savoir si la signature électronique telle qu'elle est définie par le projet de loi constitue bien une « signature avancée ». Interrogés par votre rapporteur, la Chancellerie a précisé que la directive européenne mêlait aux aspects juridiques des considérations techniques, tandis que seuls les éléments juridiques figuraient dans la définition de la signature retenue par le projet de loi, les éléments techniques étant renvoyés à un décret en Conseil d'Etat. Au total, la conjonction des dispositions du projet avec celles édictées par le futur règlement fera donc des signatures électroniques répondant aux normes françaises des signatures « avancées » au sens communautaire.

Sans entrer dans tous les détails du dispositif communautaire, notons toutefois que l'article 5 de la directive relatif aux effets juridiques des signatures électroniques dispose que ces signatures doivent être admissible en tant que preuve devant la justice. En outre, les Etats membres doivent veiller à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que *« la signature se présente sous forme électronique, qu'elle ne repose pas sur un certificat qualifié, qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature »*. Cette approche confère à la signature une présomption de fiabilité, également définie par l'article 3 du projet de loi qui dispose que *« la fiabilité de ce procédé est présumée jusqu'à preuve du 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 »*. Ce renvoi à un décret en Conseil d'Etat pour les fonctions de certification et la définition des organismes compétents pour y procéder suscite quelques interrogations sur l'architecture de cette profession.

L'article 3 de la directive précise le cadre juridique de l'exercice de la profession de certificateur. Elle interdit aux Etats membres de soumettre la fourniture de ces services à une autorisation préalable, mais leur permet d'instaurer des régimes volontaires d'accréditation tendant à améliorer le niveau de certification fourni. Elle indique à ce propos que les critères relatifs à ces régimes doivent être objectifs, transparents, proportionnés et non discriminatoires. Ensuite, la directive prévoit que chaque Etat membre veille à instaurer un système qui permette de contrôler les prestataires de service de certification établis sur son territoire et délivrant des certificats qualifiés au public. Enfin, elle ajoute que les Etats membres peuvent soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles qui doivent, d'une part, être objectives, transparentes, proportionnées et non discriminatoires et, d'autre part, ne pas constituer un obstacle aux services transfrontaliers pour les citoyens. Votre rapporteur tient à souligner tout particulièrement combien il est important que les décrets d'application relatifs à la profession de certificateur, qui devront respecter le cadre juridique dessiné par la directive, soient pris le plus rapidement possible, afin de permettre à tous les professionnels désireux d'intervenir sur ce marché de connaître les modalités pratiques de l'exercice de cette nouvelle profession.

Enfin, la directive pose dans son article 7 le principe de la non-discrimination entre les différents certificats de signature produits par les sociétés de certification. Il reviendra, en effet, aux Etats membres de veiller à ce que *« les certificats délivrés à titre de certificats qualifiés à l'intention*

du public par un prestataire de service de certification établi dans un pays tiers soient reconnus équivalents sur le plan juridique, aux certificats délivrés par un prestataire de service de certification établi dans la communauté sous certaines conditions. » Il appartiendra donc au juge de trancher entre les différents certificats, qui posséderont une valeur égale, et de déterminer lequel constitue le titre le plus vraisemblable (*cf.* l'article 1316-2 rédigé par l'article premier du projet).

III. — UN PROJET DE LOI QUI ADAPTE LE DROIT CIVIL SANS PROCEDER A UNE REVOLUTION JURIDIQUE.

En dépit du recours croissant à l'écrit électronique, les règles du doit civil font obstacle à la pleine reconnaissance de sa valeur devant le juge (A). Aussi, le projet de loi, qui adapte les règles du droit de la preuve au document numérique (B), doit-il également être complété par des moyens adéquats au profit des professions du secteur de l'écrit électronique (C).

A. LE CADRE JURIDIQUE ACTUEL FAIT OBSTACLE A LA PLEINE RECONNAISSANCE DE LA VALEUR JURIDIQUE DES ECRITS ELECTRONIQUES

« *La force des preuves par écrit consiste en ce que les hommes sont convenus de conserver par l'écriture le souvenir des choses qui se sont passées et dont ils ont voulu faire subsister la mémoire, pour s'en faire des règles, ou avoir la preuve perpétuelle de la vérité de ce que l'on a écrit* » affirmait Domat il y a plus de trois siècles au sujet de la preuve littérale. Ainsi, le droit probatoire établi par le code civil pose le principe de la supériorité de la preuve écrite préconstituée et signée qui représente le moyen de preuve parfait. En effet, en cas de contestation, il convient, pour emporter la conviction du juge, d'établir l'existence même de l'acte litigieux, d'en authentifier le contenu et d'identifier les parties. Or, si la preuve écrite préconstituée répond simultanément à ces trois préoccupations, la démonstration est moins évidente en présence de « preuves électroniques ».

1. Les exigences légales d'un écrit et d'une signature constituent un obstacle à l'admissibilité en preuve de l'écrit électronique

La preuve permet à celui qui se prévaut d'une affirmation de la faire reconnaître comme vrai et d'en tirer toutes les conséquences juridiques qui y sont attachées. Ainsi la preuve est un élément essentiel de

l'application du droit et deux grands systèmes de preuves sont généralement distingués : celui de la preuve libre et celui de la preuve légale.

Le premier laisse au juge le soin d'admettre au cas par cas si les documents qui lui sont présentés sont recevables. Dans le second, la loi guide l'intervention du juge qui est chargé de contrôler la conformité des preuves produites aux prescriptions légales. Le système français peut être qualifié de « mixte » puisque certaines branches du droit bénéficient du régime de la liberté de la preuve, comme le droit pénal ou le droit administratif, dans lequel le juge possède un pouvoir inquisitorial de recherche de la preuve. En outre, compte tenu de l'importance des flux traités dans le domaine des affaires commerciales ainsi que de la rapidité nécessaire à leur conclusion, l'article 109 du code de commerce dispose que le contrat peut être prouvé par tous les moyens. Toutefois, la preuve du commerçant contre le consommateur obéit à un régime de preuve légale afin de mieux protéger les droits de ce dernier.

Quant à l'article 1341 du code civil, il dispose : « *Il doit être passé acte devant notaire 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 témoin 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 d'une valeur moindre* ». Cet article emporte deux conséquences : d'une part, l'obligation de préconstituer une preuve écrite, sous la forme d'un acte authentique ou sous seing privé, et d'autre part, l'interdiction de prouver par témoignage contre ces actes sans qu'intervienne une quelconque limitation de valeur. Notons que le seuil prévu par cet article est fixé à 5 000 F par le décret n° 80-533 du 15 juillet 1980.

Cet article démontre clairement que l'écrit est perçu comme le meilleur moyen d'identifier la volonté de l'engagement, son contenu et sa pérennité. Pour prouver un acte juridique unilatéral, par exemple une reconnaissance de dette, il faut un écrit qui réponde aux conditions posées par l'article 1326 du code civil. Celui-ci prévoit que l'écrit doit être original, signé de la main de celui qui s'engage et doit porter la mention manuscrite de la somme ou de la quantité sur laquelle porte l'engagement en chiffres et en lettres. A défaut, l'acte irrégulier est déclassé ; sa valeur probante devient inférieure et il n'est considéré que comme un commencement de preuve par écrit. Cette dernière catégorie caractérise un écrit qui émane de la personne à qui on l'oppose et qui rend vraisemblable le fait allégué. Toutefois, le commencement de preuve constitue une modalité imparfaite de preuve qui doit être complétée par d'autres moyens probatoires comme les témoignages ou les présomptions.

Le système juridique civil français, dans son formalisme, repose donc, par son régime de preuve, sur un système séculaire d'écrit « papier », d'ailleurs parfois plus suggéré qu'expressément imposé par les textes. On ne peut s'étonner, dès lors, qu'il y ait assimilation entre l'exigence de la forme « écrite » du document et son support papier, même si le code civil ne définit nullement la notion d'écrit.

On peut aisément constater que l'écrit électronique se conforme difficilement aux exigences du code civil. L'obligation de préconstituer une preuve écrite est inadaptée à la conclusion des contrats par téléphone, aux virements bancaires, aux transactions télématiques ou par ordinateur. Les procédés numériques sont incompatibles avec les conceptions traditionnelles de l'écrit et de l'original puisque le document numérique entraîne précisément la disparition de l'original.

De plus, si un écrit obtenu par ordinateur était assimilé à un écrit, il lui manquerait toujours la signature. Or, en l'absence de définition légale de la signature, et en dépit de leur multiplication sous forme numérique, les documents électroniques signés numériquement ne sont pas recevables dans le cadre du régime de la preuve légale. Au total, les obligations de formalisme résultant des articles 1341 et 1326 du code civil ont pour effet que la *« preuve par des procédés informatiques des actes d'une valeur supérieure à 5 000 F est impossible »*. (Sophie Pennarun, de Gutenberg à Bill Gates, les petites affiches, n° 19 du 27 janvier 2000).

En examinant plus attentivement les évolutions jurisprudentielles, on peut cependant noter une évolution vers l'admissibilité en preuve de l'écrit électronique. Ainsi, la chambre commerciale de la Cour de cassation a rendu le 2 décembre 1997 une décision qui peut avoir pour effet d'assimiler un écrit électronique offrant certaines garanties à un écrit. Selon la Cour, un écrit peut être établi et conservé sur tout support, y compris par télécopie (cas de l'espèce), dès lors que son intégrité et son imputabilité à l'auteur désigné ont été vérifiées, ou ne sont pas contestées. Elle estime qu'il revient au juge d'analyser les circonstances dans lesquelles a été émis l'écrit pour établir s'il peut être retenu comme établissant la preuve d'un acte.

On le voit, cette jurisprudence constitue un pas en direction de la reconnaissance de la validité de l'écrit électronique mais celle ci demeure cependant soumise à des conditions rigoureuse qui en atténuent la portée.

La réticence du juge à l'encontre de l'écrit électronique se retrouve aussi au sein des juridictions de l'ordre administratif puisque le tribunal administratif de Rennes (28 février 1990, AJDA n° 5 p. 426) a remis en

cause le caractère probant d'une inscription à un concours par Minitel en considérant qu'à la différence de l'écrit, et à défaut de texte ou de principe général, le Minitel ne fait pas foi jusqu'à preuve du contraire.

Dans ce contexte, le législateur a tenté de réformer le droit de la preuve afin de l'adapter aux évolutions technologiques en mettant en place des régimes d'exception à la preuve écrite qui ne sont pas parfaitement satisfaisants.

2. Les exceptions légales à l'exigence d'une preuve écrite n'offrent pas un cadre juridique stable pour l'écrit électronique

La loi du 12 juillet 1980 relative à la preuve des actes juridiques a tenté de nuancer le principe de l'exigence d'un écrit par trois exceptions qui figurent aux articles 1347 et 1348 du code civil : le commencement de preuve par écrit, l'impossibilité morale de se procurer un écrit et, enfin, la faculté de recours aux copies. Ces régimes dérogatoires ont permis d'admettre l'écrit électronique en preuve, mais avec une valeur probante imparfaite.

D'abord, l'exigence d'un écrit ne s'applique pas lorsqu'il existe un commencement de preuve par écrit qui est « *un écrit qui émane de la personne à qui l'on oppose et qui rend vraisemblable le fait allégué* ». Ainsi, plutôt que d'admettre la pleine valeur probante de l'écrit numérique, il a d'abord été suggéré de le ranger dans la catégorie du commencement de preuve par écrit. A cet égard, la jurisprudence a admis qu'une caution émise par télex était un commencement de preuve par écrit. Toutefois, il convient de rappeler que le commencement de preuve n'est pas en lui-même susceptible de prouver un fait allégué. A lui seul il est inopérant et doit être complété par d'autres éléments tels que les témoignages. L'écrit électronique, en tant que commencement de preuve, demeure donc un mode de preuve imparfait.

Ensuite, l'impossibilité matérielle d'établir un écrit vaut dispense de celui-ci (article 1348 al 1). Une partie de la doctrine a soutenu (F. Chamoux, la loi du 12 juillet 1980 : une ouverture sur de nouveaux moyens de preuve, JCP éd G 1981 I n° 3008) que l'utilisation d'outils traitant l'information sous une forme dématérialisée constitue une impossibilité matérielle de produire un écrit qui reste cependant à la libre appréciation du juge. Cette analyse pour être séduisante n'en est pas moins contestable puisqu'il peut être soutenu qu'il n'est jamais impossible techniquement d'accompagner un échange électronique par un contrat écrit.

Enfin, la règle de l'écrit reçoit également exception lorsqu'une des parties ou le dépositaire n'a pas conservé le titre original mais présente une copie qui en est la reproduction non seulement fidèle mais aussi durable (article 1348 al 2). Toutefois, la référence à la copie, donc à l'existence d'un original, se prête mal aux documents numériques pour lesquels la notion même d'original n'existe plus, tandis que les manipulations sont aisées, ce qui rend délicat l'appréciation du caractère « fidèle » de la reproduction.

3. L'existence des conventions de preuve a permis à l'écrit numérique d'être admissible en preuve

Selon une jurisprudence constante, les règles de preuve ne sont pas d'ordre public, sauf dispositions légales contraires. Les parties peuvent ainsi contractuellement renoncer à l'obligation de prouver par écrit papier en signant une convention sur la preuve, le contrat étant la loi entre les parties (article 1134 du code civil).

Sous réserve de certains principes, dont le respect du débat contradictoire en cas de litige, la convention permet de renoncer par avance à l'obligation de prouver par écrit et de reconnaître certains moyens de preuve, dont les écrits numériques.

Par exemple, l'article 8-1 de la convention Carte Bleue dispose que « *les enregistrements des distributeurs de billets et appareils automatiques ou leur reproduction sur un support informatique constituent la preuve des opérations effectuées et la justification de leur imputation au compte sur lequel la carte fonctionne* ». Dès lors, la responsabilité du titulaire de la carte, partie à la convention, est engagée pour toutes les opérations faisant suite à la composition du code secret, quand bien même la carte aurait été volée.

Toutefois, le recours aux conventions de preuve doit être considéré avec une certaine prudence en raison du risque de présence de clauses abusives déséquilibrant les règles de la preuve en défaveur de l'une des parties.

Face à ces nombreuses incertitudes et compte tenu du développement des écrits et signatures numériques, l'intervention du législateur était devenue une nécessité. Cependant, avant de procéder à l'analyse du dispositif du projet de loi, il convient de rappeler que sa préparation a associé, en amont, les professionnels du secteur du commerce électronique et de la signature, mais aussi tous les citoyens désireux de s'exprimer sur ce sujet grâce aux forums organisés par le Gouvernement sur internet.

Ainsi, le forum sur l'adaptation du cadre législatif de la société de l'information organisé par le ministère des finances a recueilli 340 contributions dont 12 concernant le thème n°3 relatif à la question de la valeur probante des documents électroniques (www.finances.gouv.fr) qui témoignent à la fois d'un engouement et de craintes chez les utilisateurs.

B. LE TEXTE PROPOSE PAR LE GOUVERNEMENT CLARIFIE LA DEFINITION DE LA SIGNATURE, ASSURE LA VALEUR PROBANTE DE L'ECRIT ELECTRONIQUE TOUT EN CONFIANT AU JUGE LE SOIN DE REGLER LES CONFLITS DE PREUVE

1. Le projet de loi propose une définition de la signature qui adopte une approche neutre du point de vue des techniques employées

Comme on a pu le constater dans les développements qui précèdent, le droit français, et singulièrement le code civil, ne définissent pas la signature alors même qu'ils y font très fréquemment référence. Or, la reconnaissance de l'efficacité du document électronique comme mode de preuve serait privée de portée pratique si elle restait subordonnée à l'apposition d'une signature tracée de la main même de son auteur.

Plusieurs choix étaient possibles mais le texte a justement proposé une approche fonctionnelle de la signature. En effet, le premier alinéa du texte proposé pour l'article 1316-4 du code civil prévoit que la signature doit, d'une part, identifier celui qui l'appose et, d'autre part, manifester son consentement aux obligations qui découlent de l'acte qu'il ratifie par elle. Notons que cette définition est conforme à celle avancée par la CNUDCI.

Ensuite, le second alinéa de l'article 1316-4 précise les conditions que doivent remplir les signatures électroniques pour être dotées d'effets juridiques : « *lorsqu'elle est électronique, [la signature] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.* » En évitant de choisir une définition technique qui pourrait devenir rapidement obsolète, le projet de loi préserve l'avenir tout en insistant sur la nécessaire fiabilité du procédé.

Enfin, la dernière phrase de l'article 1316-4 instaure une présomption de fiabilité au bénéfice des signatures électroniques dès lors que « *l'identité du signataire est assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État.* »

Votre rapporteur tient à souligner, à nouveau, que ce décret concernant les modalités d'intervention des professionnels de la

certification, doit intervenir dans des délais brefs pour permettre l'émergence dans de bonnes conditions de ces nouvelles professions.

2. Le projet redéfinit la preuve littérale tout en assurant la valeur probante des documents électroniques.

Le texte proposé à l'article 1316 introduit dans le code civil, au sein du chapitre traitant de la preuve des obligations et de celle du paiement, une définition générale de la preuve littérale. Il le fait dans des termes qui couvrent tant le document écrit traditionnel sur papier que le document électronique.

Cela posé, l'article 1316-1 précise que l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier. Cette affirmation confère enfin aux documents électroniques une force probante similaire à celle de l'écrit manuscrit et fait entrer par la grande porte l'ère numérique dans le code civil. Cependant, il convient de souligner que pour être admis comme preuve le document électronique demeure soumis à des conditions tenant à l'identité de la personne dont il émane, ainsi qu'aux modalités de sa conservation qui doivent garantir son intégrité. Auditionnée par votre rapporteur, Mme Falque-Pierrotin, maître des requêtes au Conseil d'État s'est interrogée sur le fait que la recevabilité en preuve des écrits numériques soit soumise à condition, à l'inverse de la reconnaissance de la valeur probante de l'écrit numérique qui peut, en revanche, être subordonnée au respect de certaines exigences.

Enfin, pour lever l'obstacle de l'article 1326 du code civil qui impose d'écrire en chiffes, en lettres et de sa main, la somme en cause dans un acte juridique, l'article 4 du projet de loi substitue aux mots « *de sa main* » les mots « *par lui-même* ».

Afin de ne pas exclure les actes authentiques de ce mouvement de modernisation du droit civil, le Sénat a étendu à ceux-ci le bénéfice de la réalisation sous forme numérique mais pour les seuls actes *ad probationem*. Il a renvoyé les modalités pratiques de cette avancée à l'intervention d'un décret en Conseil d'État (article 1er *bis*). De même, la seconde chambre a souhaité introduire une phrase supplémentaire à l'article 1316-4 pour préciser que la signature électronique, quand elle est apposée par un officier public, « *confère l'authenticité à l'acte.* »

3. Le projet de loi confie au juge le soin de trancher les conflits de preuve

Parce que le code civil ne contient aucune disposition organisant le conflit des preuves littérales, l'article 1316-2 prévoit que lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, dont le texte consacre l'existence légale, le juge devra régler les conflits de preuve littérale en déterminant par tous les moyens le titre le plus vraisemblable, quelqu'en soit le support. Ce renvoi au juge, auquel il appartiendra de se prononcer en fonction du cas d'espèce, devrait considérablement accroître son rôle dans les années à venir.

Somme toute, si le projet de loi adapte les règles de droit civil aux exigences de l'ère numérique, votre rapporteur estime qu'il doit être complété rapidement par un cadre juridique facilitant l'émergence de professions nouvelles dans le secteur de la société d'information.

C. LES POUVOIRS PUBLICS DOIVENT VEILLER A OFFRIR UN CADRE JURIDIQUE FAVORISANT LE DEVELOPPEMENT RAPIDE DE LA CRYPTOLOGIE ET DE LA CERTIFICATION

1. Une libéralisation indispensable du régime de la cryptologie

Parce que le commerce électronique ne peut se développer sans la confiance des consommateurs et des fournisseurs, notamment en matière de télépaiement, une libéralisation du régime de la cryptologie semble nécessaire afin de compléter la reconnaissance juridique de la signature électronique par la fiabilité de sa transmission.

La cryptologie recouvre l'ensemble des techniques qui permettent de protéger des informations grâce à un code secret. L'article 28 de la loi du 29 décembre 1990 dispose qu'on *« entend par cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens matériels ou logiciels conçus à cet effet ».* Le principe de la cryptologie repose sur l'existence de « clés » de décryptage mises à la disposition du partenaire afin de lui permettre de lire clairement le message envoyé.

D'un point de vue technique, il existe aujourd'hui essentiellement deux grandes familles d'algorithmes de chiffrement : les algorithmes symétriques (à clef secrète) et les algorithmes asymétriques (à clé publique ou double clé). Les technologies de chiffrement à clé secrète permettent le

chiffrement et le déchiffrage d'un message à l'aide d'une même clé, connue des deux interlocuteurs. La puissance du chiffrement tient à la confidentialité et à la longueur de cette clé. Les technologies de chiffrement à clé publique s'appuient sur un couple de clés corrélées. L'une des clés est considérée comme publique et l'autre est conservée secrète. Le cryptage peut être utilisé soit pour masquer des données, soit pour authentifier l'émetteur ou le destinataire des données grâce à une signature électronique, soit garantir l'intégrité des données échangées.

Le chiffrement possède donc une triple fonction : d'une part interdire à un tiers de lire les informations qui ne lui sont pas destinées, d'autre part permettre au destinataire de lire ces informations, enfin s'assurer que les données reçues sont arrivées sans modifications et proviennent bien de l'émetteur. Si les méthodes de chiffrement utilisées sont incompatibles, le seul moyen sera de ne pas chiffrer. La standardisation mondiale des dispositifs utilisés pour le commerce électronique, qui doit permettre à des correspondants situés dans des pays différents de dialoguer, est donc un enjeu majeur.

En raison des intérêts que représentent les techniques de chiffrement, notamment dans le domaine de la sécurité et de la défense nationale, elles ont longtemps été soumises à des réglementations strictes. Ainsi, jusqu'en 1990, les moyens de cryptologie étaient considérés comme des armes de guerre et entraient dans le champ d'application du décret-loi du 18 avril 1939. La fabrication, le commerce et l'exportation des machines cryptographiques ne pouvaient être effectués qu'après autorisation du ministère de la Défense nationale.

La première étape de la libéralisation de la cryptologie s'est faite par la loi du 29 décembre 1990, modifiée ensuite par la loi du 26 juillet 1996. Pour autant, la question de la libéralisation de la cryptologie reste une des conditions de la croissance durable du commerce électronique. En effet, offrir des garanties quant à la sécurité des données transmises à l'occasion de la transaction électronique ne peut que favoriser l'essor global de ce type d'activité.

Tous les acteurs du commerce électronique soulignent l'importance de la mesure prise tout en souhaitant fortement que la France aille plus loin dans cette direction courageuse.

Ainsi, dans son « livre blanc », l'AFUU (Association des Utilisateurs d'Unix et de Systèmes Ouverts, www.afuu.fr), souligne que la France continue à imposer des restrictions, sans équivalent chez nos principaux partenaires commerciaux, à l'utilisation et à la

commercialisation de produits de cryptologie. Citant le cas d'une entreprise ayant délocalisé sa production en raison de la réglementation française, l'AFUU qualifie la réglementation française de « frein » au développement des sociétés. Elle ajoute que « *de nombreuses entreprises interrogées considèrent que les délais imposés par le régime de contrôle préalable des outils de cryptologie sont incompatibles avec les rythmes de leur activité économique. Aujourd'hui, malgré un raccourcissement des délais de procédure depuis les décrets de mars 1999, la complexité et la lourdeur de la constitution des dossiers techniques rallongent d'autant la mise sur le marché français de ces outils. Dans un contexte de concurrence accrue entre les entreprises, l'élément temps est d'autant plus fondamental que, dans le monde de l'informatique et des réseaux, la durée de vie d'un produit excède rarement quelques mois* ».

C'est pourquoi, votre rapporteur se félicite des annonces faites par le Premier ministre le 19 janvier 1999 dans le cadre du Comité interministériel pour la société de l'information (CISI). A cette occasion, il a fait part de la volonté du Gouvernement de substituer à la logique réglementaire de contrôle préalable des méthodes de cryptage, une logique de contrôle *a posteriori*, basée sur des moyens de poursuite de leur utilisation illicite afin de préserver la capacité d'action et de répression des pouvoirs publics. A cet égard, le Conseil de l'Europe a bien mis en évidence la nécessité de trouver un équilibre entre les contraintes commerciales et celles liées aux considérations d'ordre public (recommandation R. 95-13 du 11 septembre 1995).

D'un point de vue chronologique, la libéralisation de l'usage de la cryptologie, telle qu'elle a été annoncée par le Gouvernement, devrait se poursuivre en deux temps.

Il a d'abord été procédé à une redéfinition de la forme et du contenu des déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie. Cette étape, marquée par les décrets n^{os} 199 et 200 du 17 mars 1999, a permis d'élever le niveau de sécurité des outils de cryptologie autorisés en France en allégeant les formalités administratives. A ce jour, les procédures à suivre varient selon la puissance du chiffrement. Sommairement, les moyens de chiffrement, qui ne dépassent pas 128 bits et sont destinés à assurer la confidentialité, sont d'utilisation et d'importation libre, tandis que leur exportation reste soumise à autorisation préalable. En ce qui concerne les moyens de chiffrement supérieurs à 128 bits, le régime applicable est plus restrictif : leur fourniture, leur exportation et leur importation sont soumises à autorisation préalable ; leur utilisation est également soumise à autorisation préalable, à moins que les utilisateurs ne séquestrent leurs clés de chiffrement auprès d'un tiers de confiance agréé

par le Gouvernement. Le tiers de confiance, dont la fonction est de conserver les clés de chiffrement, est soumis à des obligations légales de remise ou de mise en œuvre de celles-ci à la demande des autorités judiciaires ou de sécurité. Ainsi, lorsque les conditions prévues par le code de procédure pénale ou par la loi du 10 juillet 1990 sur les interceptions téléphoniques sont remplies, le tiers de confiance peut se voir obligé de remettre les clés aux autorités publiques qui ont ainsi accès à tout moment aux textes en clair. Notons toutefois que les textes réglementaires comportent une ambiguïté que certains experts, dont M. Jacques Stern, ont souligné devant votre rapporteur. En effet, le principe de la double clé asymétrique fait que techniquement une signature chiffrée à hauteur de 128 bits exige une clé publique largement plus longue donc supérieure au seuil défini par le décret du 17 mars 1999.

Une seconde étape devrait prendre la forme de dispositions qu'il conviendra d'inscrire dans le futur projet de loi relatif à la société de l'information. Ce texte pourrait être l'occasion de mettre en œuvre un régime de chiffrement plus libéral qui ne désarmerait pas pour autant l'Etat face à des utilisations dangereuses et qui pourrait, par ailleurs, prendre en compte d'autres moyens d'identification des messages comme le recours à l'iris de l'œil et à la biométrie. Sans doute devra-t-il également, comme le Gouvernement semble vouloir s'y engager, de passer d'un recours obligatoire à un recours facultatif au tiers de confiance.

2. Une réglementation attendue de l'offre de service de certification

En complément du recours au chiffrement, le développement du commerce électronique peut conduire à l'élaboration de mécanismes destinés à gérer les questions de preuve au travers de la désignation, par les parties, d'un tiers authentificateur qui tient son pouvoir de celles ci et non de la loi.

Un tiers certificateur doit pouvoir proposer les services suivants ; l'identification fiable de l'émetteur et du destinataire, l'intégrité des données transmises, le contrôle des non-répudiations par l'émetteur et le destinataire des données transmises, la mise en place d'un système de preuve opérationnel qui implique la conservation de celles-ci au moyen de la trace électronique laissée par le message et enfin la certification des échanges par un horodatage complet. Votre rapporteur tient à faire remarquer que La Poste travaille d'ores et déjà à l'élaboration de différents services de certification, qui constituent une extension dans le domaine numérique de ses activités traditionnelles ; ainsi, l'horodatage est-il

l'équivalent du cachet de la poste, tandis que le transport de documents dont l'intégrité est garantie se rapproche du courrier, métier traditionnel de l'exploitant public.

Si le tiers certificateur est chargé d'établir la preuve en cas de litige entre deux utilisateurs d'un service de télétransmission, des litiges peuvent également naître entre les utilisateurs et l'organisme certificateur. Dans un tel cas, ce dernier doit pouvoir rapporter la preuve que le service a bien été rendu. Rencontrée par votre rapporteur, La Poste a tenu à souligner que les quelques prestataires de certification actuels étant des multinationales, cette situation pourrait, en cas de contentieux, conduire à la dilution des responsabilités au niveau mondial et présenter, de ce fait, des difficultés juridiques importantes pour les particuliers.

L'article 3 du projet de loi dispose que la fiabilité du procédé de la signature est présumée lorsque l'identité du signataire et l'intégrité de l'acte sont garanties dans des conditions fixées par décret en Conseil d'État. Ce renvoi au pouvoir réglementaire pour la détermination des modalités pratiques d'intervention des certificateurs présente l'avantage de ne pas fixer dans la loi des conditions techniques pouvant devenir rapidement obsolètes. Toutefois, on peut remarquer que les annexes I et II de la directive sur la signature électronique fournissent au pouvoir réglementaire un cadre assez précis quant à la nature des certificats et aux exigences concernant les prestataires de service.

En ce qui concerne les certificats qualifiés, l'annexe I de la directive précise notamment qu'ils doivent comporter : l'identification du prestataire de certification ainsi que le pays dans lequel il est établi, le nom du signataire, mais aussi les données afférentes à la vérification de la signature du signataire, l'indication du début et de la fin de la période de validité du certificat ainsi que les limites éventuelles à la valeur des transactions pour lesquelles le certificat peut être utilisé.

Pour ce qui est des certificateurs, rappelons que leur accès au marché communautaire n'est soumis à aucune autorisation préalable (article 2 de la directive), ce qui n'exclut pas des mesures de contrôle de la part d'une autorité, qu'elle soit publique ou privée. De surcroît, l'annexe II apporte des précisions qui devraient permettre une publication rapide des décrets d'application.

Aux termes de cette annexe, les prestataires de certification doivent notamment : faire la preuve qu'ils sont suffisamment fiables pour fournir un tel service, assurer le fonctionnement d'un service d'annuaire et de révocation rapides et sûrs, veiller à ce que la date et l'heure d'émission et de

révocation d'un certificat puissent être déterminées avec précision, vérifier par des moyens appropriés et conformes au droit national l'identité et les qualités spécifiques de la personne à laquelle un certificat est délivré.

Par ailleurs, les certificateurs doivent utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable, de sorte que l'information puisse être contrôlée quant à son authenticité et que toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

Sur ce dernier point votre rapporteur tient à souligner l'enjeu que constitue la question de la conservation durable des certificats et des documents numériques en règle générale. Dans une optique de long terme, l'évolution des supports numériques commande de distinguer clairement l'information, qui doit être durable et intégralement conservée, des modalités pratiques de sa conservation qui doivent nécessairement être actualisables et modifiables.

*

* *

Après l'exposé du rapporteur, plusieurs commissaires sont intervenus dans la discussion générale.

M. Olivier de Chazeaux a estimé que le projet de loi allait dans le bon sens en permettant l'adaptation du droit de la preuve à la nouvelle économie qui émerge grâce au développement de nouveaux modes de communication. Il a néanmoins appelé à une grande vigilance, lors de la rédaction des textes tirant les conséquences de ces nouvelles technologies, en raison du phénomène du piratage. Il a souligné que, en l'état, la législation française ne permettait pas d'utiliser en toute sécurité juridique le support électronique, notamment comme mode de preuve, et que les entreprises appelaient de leurs vœux une sécurisation juridique et technique qui, loin d'entraver les échanges commerciaux devrait au contraire favoriser leur développement. Tout en souhaitant que les actes authentiques ne restent pas à l'écart de cette modernisation, il a rappelé que, aux termes de l'article 1317, ces actes étaient reçus « *avec les solennités requises* », ce qui suppose notamment la présence de l'officier public. Il s'est interrogé sur le contenu du décret en Conseil d'Etat chargé de préciser les conditions dans lesquelles serait établi et conservé un acte authentique dressé sur support électronique et a jugé indispensable que la garde des sceaux apporte des précisions à ce sujet lors du débat en séance. Par ailleurs, il a souhaité que la dématérialisation de ces actes ne se traduise pas, à terme, par une suppression de la fonction d'officier public.

M. Alain Vidalies a observé que la nécessité d'une réforme du droit de la preuve était largement admise, le code civil ayant été rédigé à une époque où le seul support des actes juridiques était le papier. Faisant référence à un arrêt de la Chambre commerciale de la Cour de cassation, en date du 2 décembre 1997, il a souligné que le projet de loi tirait les conséquences d'une évolution jurisprudentielle sur l'admissibilité de l'écrit en preuve. Il a rappelé que, si le projet répondait certes à une exigence européenne, la France, avant même l'adoption de la directive du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, avait souhaité reconnaître dans le code civil la validité de la signature électronique. Concernant les actes authentiques, il s'est interrogé sur l'introduction dans le code civil d'une disposition s'apparentant à un effet d'annonce, dont les délais de mise en œuvre restent incertains, la rédaction des décrets présentant d'autant plus de difficulté que les actes authentiques ne se résument pas aux actes notariés. Il a donc souhaité que l'introduction dans le code civil de la possibilité de dresser un acte authentique sur support électronique s'accompagne de davantage de précisions, une simple pétition de principe ne pouvant satisfaire le législateur.

M. Claude Goasguen a souligné que la reconnaissance de l'écrit électronique et de la signature électronique était attendue de longue date par les milieux d'affaires. Il s'est inquiété des délais de publication du décret en Conseil d'Etat chargé de fixer les conditions de fiabilité de la signature électronique et s'est interrogé sur la compatibilité des normes européennes avec celles reconnues aux Etats–Unis et dans les pays asiatiques. Il a estimé qu'un équilibre devait être trouvé entre la nécessaire sécurité des transactions et la liberté des échanges, afin que les entreprises françaises ne soient pas handicapées par rapport à leurs concurrents internationaux. Enfin, il a considéré que la possibilité de dresser des actes authentiques sur support électronique devrait conduire à supprimer la référence aux « solennités requises » mentionnées par l'article 1317 du code civil. Après avoir souligné le travail remarquable accompli par le Conseil d'Etat sur les questions d'ordre juridique posées par le développement d'Internet, **M. Martin-Lalande** a souhaité que le développement des téléprocédures dans les collectivités territoriales et plus généralement dans l'administration soit encouragé, notamment pour les décisions des autorités délibérantes et les procédures de marchés publics. Enfin, il a insisté sur la sécurité en matière de datation des actes électroniques.

M. Gérard Gouzes a souligné combien il était nécessaire de clarifier la situation juridique de l'écrit électronique, la doctrine comme la jurisprudence n'apportant pas aujourd'hui de réponse univoque.

En réponse aux intervenants, le rapporteur a apporté les précisions suivantes.

— Il serait inexact d'affirmer que la France est en retard dans la course contre le temps qui est imposée à tous les Etats par le développement de la société de l'information. Il est d'ailleurs significatif que le texte du projet de loi relatif au droit de la preuve et à la signature électronique ait été examiné par le Conseil des ministres avant même que la directive du 13 décembre 1999 n'ait été adoptée par le Conseil de l'Union européenne.

— Cette avance ne saurait être annihilée par une quelconque lenteur dans l'élaboration des textes d'application de la nouvelle loi. Le Gouvernement devra veiller à la célérité du travail de l'administration. En particulier, le décret en Conseil d'Etat relatif à la certification devra être publié dans les plus brefs délais, afin que le développement de ce nouveau procédé technologique ne soit pas entravé par des pesanteurs administratives : le Conseil d'Etat possède toutes les compétences et les capacités d'expertise nécessaires pour mener à bien ce travail, s'agissant d'un domaine où il a prouvé, en 1998, à travers son rapport sur « Internet et les réseaux numériques », qu'il n'était nullement en retard. En ce qui

concerne le décret sur les actes authentiques sur support numérique, il serait certainement utile que le Gouvernement fournisse au Parlement un certain nombre de précisions relatives aux orientations qu'il entend privilégier. Ainsi, les textes réglementaires devront avoir une portée « prospective », de façon à prendre en compte le développement potentiel de procédés expérimentaux nouveaux permettant de s'assurer du consentement des parties, tels que les vidéoconférences et les technologies de biométrie.

— S'agissant de la dimension internationale, il faut souligner que le projet de loi n'est pas le résultat d'un travail « franco-français ». Il s'inscrit dans le cadre d'une directive européenne et il n'est pas sans lien avec les réflexions menées, en matière de signature électronique, au sein de la commission des Nations Unies pour le droit commercial international (CNUDCI).

— Les dispositions qu'il tend à mettre en œuvre sont de nature à satisfaire les consommateurs, qui réclament plus de sécurité et de confiance pour utiliser en confiance les procédés informatiques à des fins commerciales. C'est pourquoi, dans ce domaine, il n'est pas pertinent d'opposer la liberté et la sécurité des échanges, bien qu'il s'agisse d'un débat ancien entre la majorité et l'opposition parlementaire : la sécurisation de la signature électronique supprimera une entrave majeure au développement du marché électronique et pourrait conférer à la France en particulier, et à l'Europe en général, un avantage déterminant dans la compétition qui les oppose aux Etats-Unis.

— En matière de sécurité, le projet de loi réalise une avancée décisive en conférant à l'écrit électronique une force probante équivalente à celle de l'écrit papier, alors qu'il ne constituait jusqu'à présent, au mieux, qu'un commencement de preuve. S'agissant des actes authentiques, ce caractère probatoire est absolu : il s'appliquera à tous les actes authentiques, qu'ils soient accomplis par les notaires, les officiers d'état civil, les préfets ou les huissiers.

— L'application des dispositions nouvelles du projet de loi aux actes authentiques réalisés par les officiers d'état civil montre, d'ailleurs, que bien que ce texte ne concerne, en principe, que les relations entre les parties privées, il contient néanmoins un certain nombre d'éléments qui vont dans le sens d'une modernisation des relations qui unissent l'Etat et les citoyens. A cet égard, des expérimentations importantes, qui concourent à la dématérialisation des procédures publiques, sont également en cours, y compris en matière d'urbanisme, voire de contrôle de légalité. Dès le début de l'année 2001, les entreprises pourront utiliser la voie électronique pour transmettre à l'administration leurs déclarations d'échanges de biens ou

pour s'acquitter de la TVA. La réflexion n'est donc pas abstraite et ses applications se manifesteront de façon croissante dans la pratique quotidienne des usagers.

— Le succès de cette démarche suppose le développement concomitant d'un certain nombre de procédés technologiques. Ainsi, il conviendra d'améliorer les systèmes de cryptologie, mais aussi de datation numérique. Des techniques équivalentes au « cachet de la poste » sont sur le point d'être mises au point.

*

* *

EXAMEN DES ARTICLES

L'utilisation croissante des moyens électroniques de communication se traduit par une disparition du support papier, tant pour l'élaboration que pour la transmission des documents. Ainsi, quand une offre est formulée par courrier électronique et que son destinataire répond par le même moyen, le contrat est formé. Mais l'écrit, au lieu de figurer sur une feuille de papier, sera reproduit sur l'écran, puis éventuellement tiré sur l'imprimante, et le « facteur » sera le fournisseur d'accès à Internet. Mais, en cas de contestation, comment préconstituer une preuve ? La dématérialisation des documents rend, en effet, nécessaire une adaptation du code civil qui, depuis ses origines, pose comme principe la supériorité de la preuve écrite préconstituée et signée.

En cas de contestation d'un acte juridique, il est nécessaire d'établir l'existence de l'acte litigieux, d'en authentifier le contenu et d'identifier les parties. En droit civil, le juge ne peut former sa conviction que d'après les moyens de preuve admis par la loi et la preuve écrite, préconstituée et signée, a une valeur supérieure aux autres formes de preuve (preuve par témoin, par présomption, par aveu ou par serment). La dématérialisation des documents, qui conduit à la disparition du papier et à son remplacement par d'autres supports, impose une « dématérialisation de la preuve » et donc une indispensable adaptation des dispositions du code civil en raison de l'importance, en nombre et en valeur, que prendront les contrats électroniques dans un proche avenir. Les questions que pose la preuve des obligations et du paiement ne se limitent pas aux documents eux-mêmes, elles s'étendent aux problèmes d'archivage.

Au sein du livre troisième du code civil relatif aux « différentes manières dont on acquiert la propriété », le titre III traite « des contrats ou des obligations conventionnelles en général ». Les règles relatives à la preuve des obligations sont précisées par le chapitre VI, lui-même découpé en cinq sections portant sur la preuve littérale (section I), la preuve testimoniale (section II), les présomptions (section III), l'aveu de la partie (section IV) et le serment (section V).

Afin que le contrat sur support électronique puisse devenir un mode alternatif de conclusion des conventions, apportant la même sécurité juridique que le support papier, le présent projet adapte les règles relatives à la preuve littérale à l'environnement électronique et, plus précisément, celles contenues dans les deux premiers paragraphes relatifs au titre

authentique et à l'acte sous seing privé, les paragraphes traitant des tailles, des copies, des titres et des actes récognitifs et confirmatifs demeurant inchangés.

Le projet tend à reconnaître la valeur probatoire du document électronique. A cette fin, l'article premier définit l'écrit sans tenir compte de son support, reconnaît l'admissibilité comme mode de preuve du document électronique et confie au juge le soin de régler les confits de preuve littérale. L'article 2 accorde à l'écrit électronique la même force probante qu'à l'écrit sur support papier. L'article 3 définit la signature et traite du cas où la signature est électronique.

Le Sénat a approuvé ces dispositions, sous réserve de modifications rédactionnelles. Il a, en outre, introduit un article 1er *bis* tendant à faire figurer dans la loi le principe selon lequel l'acte authentique peut être dématérialisé et sa signature apposée sous la forme électronique. En conséquence, il a procédé à des modifications de référence, les nouveaux articles du code civil relatifs à la force probante et à la signature étant sortis du paragraphe relatif à l'acte sous seing privé pour être insérés dans le paragraphe contenant les dispositions générales en matière de preuve littérale : les articles 1322-1 et 1322-2 du code civil sont donc devenus les articles 1316-3 et 1316-4 dans le texte du Sénat.

ARCHITECTURE DE LA SECTION I DU CHAPITRE VII DU TITRE III DU LIVRE TROISIEME DU CODE CIVIL

Dans le texte en vigueur	Dans le texte du projet de loi	Dans le texte adopté par le Sénat
CHAPITRE VI **De la preuve des obligations** – art. 1315 – art. 1316	CHAPITRE VI **De la preuve des obligations** – art. 1315 – art. 1315-1	CHAPITRE VI **De la preuve des obligations** – art. 1315 – art. 1315-1
Section I ***De la preuve littérale***	*Section I* ***De la preuve littérale***	*Section I* ***De la preuve littérale***
	§ 1er : Dispositions générales – art. 1316 à 1316-2	**§ 1er : Dispositions générales** – art. 1316 à 1316-2 – ***art. 1316-3 et 1316-4***
§ 1er : Du titre authentique – art. 1317 à 1321	**§ 2 : Du titre authentique** – art. 1317 à 1321	**§ 2 : Du titre authentique** – art. 1317 à 1321
§ 2 : De l'acte sous seing privé – art. 1322 – art. 1323 à 1332	**§ 3 : De l'acte sous seing privé** – art. 1322 – ***art. 1322-1 et 1322-2*** – art. 1323 à 1332	**§ 3 : De l'acte sous seing privé** – art. 1322 – art. 1323 à 1332

Article premier

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

Reconnaissance de la valeur juridique du document électronique

Cet article comporte trois paragraphes adoptés sans modification par le Sénat, sous réserve d'une précision rédactionnelle dans le dernier paragraphe.

Le chapitre du code civil relatif à la preuve des obligations et du paiement s'ouvre sur deux articles généraux communs à tous les modes de preuve, l'article 1315 relatif à la charge de la preuve et l'article 1316 qui annonce les cinq sections du chapitre portant respectivement sur la preuve littérale, la preuve testimoniale, les présomptions, l'aveu de la partie et le serment. L'article premier du projet procède à un réaménagement de la section relative à la preuve littérale, qui se traduit par des changements de références et l'introduction de nouvelles dispositions.

Sur la forme, l'article 1316 devient l'article 1315-1, mais ni son emplacement ni son contenu ne sont modifiés, et un nouveau paragraphe comportant des dispositions générales est inséré en tête de la section relative à la preuve littérale (art. 1316 à 1316-2 *nouveaux*) ; en conséquence, les actuels paragraphes 1er à 5 deviennent les paragraphes 2 à 6.

Sur le fond, les nouvelles dispositions de l'article 1316 et les nouveaux articles 1316-1 et 1316-2 font de l'écriture électronique l'une des formes légalement reconnues de la preuve littérale : les nouvelles technologies effacent les frontières entre supports et laisse au contenu le rôle central,

La définition donnée à la preuve littérale couvre aussi bien le document électronique que l'écrit traditionnel sur support papier (art. 1316)

Actuellement, la preuve littérale ou preuve par écrit n'est pas définie tant il était évident, lors de la rédaction du code civil et il y a peu de temps encore, que l'adjectif littéral désignait « une écriture apposée en signes lisibles sur un support tangible ». Afin de tenir compte de l'évolution de la nature de l'écrit, et de pouvoir en tirer toutes les conséquences juridiques, le projet définit la preuve par écrit dans des termes suffisamment généraux pour couvrir aussi bien l'écrit traditionnel sur support papier que l'écrit électronique.

Aux termes de cette définition, la preuve écrite se présente comme une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles (logos, par exemple). Sur le fond, cette suite de signes doit être dotée d'une signification intelligible : en conséquence, un texte crypté, mais déchiffrable par son destinataire, est intelligible et possède donc une vocation probatoire. Il n'y a aucune autre condition requise et notamment aucune condition tenant au support ou aux modalités de transmission : la preuve littérale ne s'identifie plus au papier et peut résulter d'une communication à distance (e-mail, disquette, disque dur, …).

Ainsi que le souligne l'exposé des motifs du projet de loi, cette définition de l'écrit, dont il résulte que le support numérique est un écrit comme l'est le papier, est placée en tête de la section relative à la preuve littérale et ne concerne donc que l'écrit exigé *ad probationem* et reste sans incidence sur l'écrit exigé *ad solemnitatem*.

*L'écrit électronique est admis comme mode de preuve au même titre que l'écrit sur support papier (*art. 1316-1 *nouveau).*

La notion d'écrit étant refondée, le support numérique est-il admissible comme mode de preuve et, si oui, quelle valeur probatoire lui accorde-t-on ? Ni plus ni moins qu'à l'écrit dans un environnement papier, répond le projet de loi.

Adopté sans modification par le Sénat, l'article 1316-1 *nouveau* précise que l'écrit sous forme électronique, quel qu'il soit, est admis en preuve au même titre que l'écrit sur support papier. Toutefois, en raison de l'introduction d'une dimension technique tenant au support numérique, deux conditions sont mises à l'admission de l'écrit électronique comme mode de preuve de même rang que l'écrit traditionnel : celui dont il émane doit pouvoir être identifié et les modalités de conservation doivent garantir son intégrité. Il s'agit là de la transposition légale d'un arrêt de la Cour de cassation (Cass., com., 2 décembre 1997), rendu à propos de la valeur d'une télécopie : « *l'écrit (...) peut être établi et conservé sur tout support, y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées ».* En effet, avec le support électronique, le problème n'est pas entièrement juridique, il est également technique : sur le plan technique, il faut en effet que le degré de fiabilité du document soit le plus grand possible pour offrir les garanties nécessaires.

Si les moyens techniques utilisés donnent des assurances sur l'imputabilité et la conservation durable du document, l'écrit électronique est donc admis en preuve dans des conditions identiques à un écrit sur

support papier. Ainsi, dès lors que des garanties existent sur l'authenticité et l'intégrité du message, l'écrit numérique vaudra preuve, qu'il s'agisse d'un échange de correspondance électronique, d'un accord matérialisé dans un cédérom ou encore d'un achat en ligne dans le E-business. Comme l'a écrit le professeur Pierre-Yves Gautier, « *peu importe le support, pourvu qu'on ait la certitude* ».

Il revient au juge de régler les conflits de preuve littérale (art. 1316-2 nouveau).

Des conflits entre preuves littérales peuvent surgir, par exemple si un support papier signé entre les parties est en conflit avec un écrit numérique qui le contredit ou si deux actes électroniques sont produits.

Adopté sans modification par le Sénat, l'article 1316-2 *nouveau* précise que, sauf dispositions légales ou conventionnelles contraires, les tribunaux règlent les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. Il s'agit là de la confirmation d'une jurisprudence constante, selon laquelle les règles de la preuve ne sont pas d'ordre public sauf dispositions légales contraires et c'est pourquoi les parties peuvent renoncer à l'obligation de preuve par écrit en signant une convention sur la preuve.

Cet article a donc un caractère supplétif puisqu'il n'a vocation à s'appliquer que « *lorsque la loi n'a pas fixé d'autres principes* », qui organiseraient une hiérarchie des forces probantes, comme cela existe déjà dans notre législation : ainsi, la somme écrite en lettres l'emporte sur celle écrite en chiffres en cas de différence (cf. art. 1326 du code civil relatif aux actes sous seing privé), les mentions des actes authentiques ont une force probante renforcée, … Il sera donc possible d'élaborer des régimes particuliers en fonction des mutations techniques améliorant la fiabilité des modes de communication et de conservation des écrits numériques.

Par ailleurs, cet article ménage aux parties la possibilité de recourir à des conventions sur la preuve pour prévenir les conflits de preuve littérale et dérogeant aux règles supplétives contenues dans le code civil. La valeur probatoire de la convention des parties, déjà admise par la jurisprudence mais avec certaines incertitudes, est ainsi clairement reconnue par la loi. La validité de la convention reste néanmoins soumise à l'appréciation du juge, car elle ne saurait déroger à des règles légales impératives, par exemple celles concernant la force probante des actes authentiques, ou à une règle substantielle de l'administration judiciaire de la preuve comme le respect du contradictoire.

A défaut de règle légale et de convention valable entre les parties, le juge aura toute liberté pour régler les conflits de preuves, en fonction des circonstances de l'espèce et déterminer le titre le plus vraisemblable « quel qu'en soit le support », puisqu'il n'y a pas de hiérarchie probante entre les écrits en fonction de leur support. La notion de vraisemblance est déjà connue du droit de la preuve, l'article 1347 du code civil définissant le commencement de preuve par écrit comme l'écrit qui rend vraisemblable le fait allégué.

La Commission a *adopté* l'article premier sans modification.

Article 1er bis (nouveau)

(art. 1317 du code civil)

Possibilité de dresser des actes authentiques sur support électronique

Introduit par le Sénat avec l'avis favorable du Gouvernement, cet article complète l'article 1317 du code civil, qui définit l'acte authentique, afin de préciser que cet acte peut être dressé sur support électronique, s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. Il ne s'agit pas là d'encadrer une pratique, mais plutôt d'ouvrir un cadre légal pour l'avenir. Le code civil place en tête de la hiérarchie des preuves par écrit l'acte authentique suivi de l'acte sous seing privé.

Aux termes de l'article 1317 du code civil, l'acte authentique est un écrit établi par un officier public avec les solennités requises. La qualité d'officier public est conférée aux personnes qui ont le pouvoir d'authentifier des actes : le maire en tant qu'officier de l'état civil, le greffier du tribunal de commerce, l'huissier de justice, le notaire…

Comme l'acte sous seing privé, l'acte authentique est un acte instrumentaire, c'est-à-dire un écrit rédigé spécialement en vue de constater des droits et obligations. Mais, à la différence de l'acte sous seing privé, il est revêtu d'une qualité particulière, l'authenticité, résultant de ce qu'il est dressé par un officier public (ce qui impose sa présence pour recevoir le consentement des parties) suivant les formalités requises. Ces formalités varient selon les catégories d'actes, mais deux formalités sont toujours exigées : la signature manuscrite de l'officier public et l'indication de la date.

L'acte authentique est revêtu d'une force probante particulière, puiqu'il fait foi jusqu'à inscription en faux des faits que l'officier public y a énoncés : il ne peut être contesté que dans le cadre de cette procédure

spécifique obéissant à des règles très précises (art. 303 et suivants du nouveau code de procédure civile). Par ailleurs, les grosses de l'acte authentique (les copies revêtues de la formule exécutoire) sont susceptibles d'exécution forcée.

Aux termes de l'article 1322 du code civil, l'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a entre ceux qui l'ont souscrit la même foi que l'acte authentique. 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. Il 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. S'il s'élève une contestation relative à un acte sous seing privé, il appartient au juge de procéder à la vérification d'écriture conformément aux dispositions des articles 287 et suivants du nouveau code de procédure civile. 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.

S'il est évident que l'acte authentique ne saurait rester en dehors de la révolution numérique, c'est une chose d'affirmer qu'il peut être dématérialisé et sa signature apposée sous forme électronique, c'en est une autre de rendre effective cette affirmation. En effet, ainsi que l'a souligné la garde des sceaux au Sénat, les mesures techniques permettant la dématérialisation des actes authentiques ne peuvent être mises en place dans l'immédiat, les réponses à apporter aux nombreuses questions qui se posent nécessitant une réflexion préalable approfondie. La ministre a d'ailleurs indiqué qu'elle entendait confier à un groupe de travail réunissant des juristes et des experts en technologies nouvelles le soin d'étudier les mesures nécessaires.

Les difficultés sont d'autant plus nombreuses que, contrairement à ce que l'on pourrait croire, les actes authentiques ne se résument pas aux actes notariés (contrat de mariage, donation, vente d'immeuble, …). Il existe, en effet, une grande variété d'actes authentiques, avec autant de régimes particuliers et de contraintes spécifiques. Sont ainsi concernés par une éventuelle dématérialisation :

- les actes de l'état civil ;
- les jugements :
- les actes dressés par les huissiers dans l'exercice de leurs attributions légales ;

– les procès-verbaux dressés par les commissaires-priseurs ;

– certains procès-verbaux dressés par les officiers de police judiciaire (en matière douanière, forestière ou de pêche fluviale) ;

– certains actes publics établis par les préfets, sous-préfets, maires et adjoints dans l'exercice de leurs fonctions ;

– les procès-verbaux des experts et autres techniciens.

C'est dire que l'élaboration des décrets tirant les conséquences, domaine par domaine, de la possibilité de dresser des actes authentiques sans support papier sera particulièrement complexe.

Comme l'a souligné le rapporteur de la commission des lois du Sénat, cette faculté ne modifie aucunement le formalisme de l'acte authentique : cet acte « *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* ».

La Commission a *adopté* l'article premier *bis (nouveau)* sans modification.

Article 2

(art. 1316-2 du code civil)

Force probante de l'écrit sur support électronique

Une fois affirmé que l'écrit électronique est admis en preuve au même titre que l'écrit sur support papier (art. 1er du projet), se pose la question de sa force probante.

Adopté par le Sénat dans son principe, le présent article reconnaît à l'écrit électronique la même force probante qu'à l'écrit sur support papier. Fidèle à sa logique, le projet n'instaure pas de hiérarchie des écrits : le papier ne l'emporte pas sur le numérique, ce qui aurait été un frein au développement des contrats en ligne.

Initialement insérée dans le paragraphe du code civil relatif à l'acte sous seing privé (art. 1322-1), cette disposition a été transférée par le Sénat dans le nouveau paragraphe 1er comportant des dispositions générales sur la preuve littérale.

Par ailleurs, à la demande du Gouvernement, le Sénat a renoncé à préciser que l'écrit électronique n'a une force probante équivalente à celle de l'écrit sur support papier que s'il « *réunit toutes les conditions de forme nécessaire à sa validité* ». En effet, cette mention particulière pouvait laissait croire à une remise en cause du principe d'équivalence entre les supports. En outre, comme l'a souligné la garde des sceaux, il va de soi que l'écrit électronique ne peut se voir reconnaître une valeur probante identique à l'écrit sur support papier que s'il remplit les mêmes conditions de forme que celles exigées pour ce type d'écrit : ainsi, lorsqu'il sera signé et aura été préétabli pour constater des droits et des obligations, l'acte sur support électronique aura la force probante d'un acte sous seing privé et ne pourra être combattu que par un autre acte, authentique ou sous seing privé.

C'est pourquoi, le Sénat a supprimé une disposition superflue figurant dans le texte initial du projet et tendant à préciser que la force probante reconnue à l'acte authentique ne valait que « *lorsqu'il constate des droits et obligations et qu'il est signé* » : seuls sont concernés par le présent article les actes juridiques créateurs de droits et d'obligations et la signature de ceux qui s'obligent est une condition de forme commune aux actes authentiques ainsi qu'aux actes sous seing privé.

La Commission a *adopté* l'article 2 sans modification.

Article 3

(art. 1316-4 du code civil)

Fonctions de la signature
Force probante de la signature électronique

La valeur probatoire de l'écrit électronique étant reconnue, le présent article définit les fonctions de la signature, la signature étant une condition d'existence de l'acte instrumentaire, et admet qu'une signature puisse être effectuée sous forme électronique. Sous réserve d'une modification purement rédactionnelle, le Sénat a adopté les dispositions de cet article dans la rédaction élaborée par le Gouvernement après les avoir complétées par un alinéa relatif à l'apposition de la signature par un officier public. Par ailleurs, comme à l'article précédent relatif à la force probante de l'écrit électronique, il a transféré les dispositions du présent article dans le paragraphe consacré aux dispositions générales en matière de preuve littérale, alors qu'elles étaient initialement placées dans le paragraphe relatif aux actes sous seing privé.

Alors même que notre droit positif impose fréquemment qu'un acte soit signé, les rédacteurs du code civil n'ont pas jugé utile de définir la

signature tant il leur paraissait évident qu'il s'agissait de l'apposition manuelle d'un signe distinctif sur un support tangible, de même qu'ils n'ont pas éprouvé le besoin de définir l'écrit confondu avec le support papier. Mais l'entrée dans l'ère numérique a suscité l'apparition d'un équivalent électronique à la signature manuscrite, en même temps qu'elle a dématérialisé l'écrit, et rendu nécessaires des définitions générales et abstraites de l'écrit et de la signature.

Comme le souligne l'exposé des motifs du projet de loi, « *la reconnaissance de l'efficacité du document électronique comme mode de preuve serait privée de portée pratique si elle restait subordonnée à l'apposition sur celui-ci d'une signature tracée de la main même de son auteur* ». C'est pourquoi, la directive européenne du 13 décembre 1999 impose aux Etats membres de reconnaître la validité juridique de ces nouveaux procédés de signature, qui apportent la fiabilité nécessaire à la sécurité des transactions grâce au développement des techniques de cryptologie et de certification.

Le premier alinéa du présent article ne définit pas à proprement parler la signature nécessaire à la perfection d'un acte. Conformément à l'approche préconisée par la CNUDCI, il énonce sa double fonction en matière de preuve, qu'elle soit manuscrite ou électronique : identification de celui qui l'appose et manifestation de son consentement aux obligations découlant de l'acte. Il y a donc une « équivalence fonctionnelle » entre signature manuscrite et signature électronique, cette signature étant « avancée » au sens de la directive européenne. Le Sénat a, par ailleurs, précisé que l'apposition de la signature par un officier public confère l'authenticité à l'acte lui-même.

Aux termes du deuxième alinéa de cet article, lorsqu'elle est électronique, la signature consiste en « l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache », de telle sorte que toute modification ultérieure des données soit détectable : conformément aux prescriptions de la directive, ces termes sont suffisamment généraux pour laisser place à toutes les modalités techniques existantes, ou à venir, satisfaisant aux conditions posées dans le code civil.

Par ailleurs, conformément à la directive précitée, il est institué une présomption de fiabilité de la signature électronique, jusqu'à preuve du contraire (qui sera relativement difficile à rapporter), lorsque l'identité du signataire est assurée et l'intégrité de l'acte garantie. Ces exigences de fiabilité seront définies, en fonction des évolutions techniques, par un décret en Conseil d'Etat qui encadrera l'intervention des prestataires de services de

certification conformément aux exigences techniques énoncées dans les annexes de la directive.

Le prestataire de services de certification authentifie le signataire mais ne certifie pas le contenu du message, à la différence de l'officier public : au sens technique, l'authentification ne porte jamais sur le contenu des actes juridiques et, d'ailleurs, le tiers certificateur ne connaît pas le contenu du message certifié.

La Commission a *adopté* l'article 3 sans modification.

Article 4

(art. 1326 du code civil)

Mentions manuscrites

Adopté sans modification par le Sénat, cet article a pour objet de lever un obstacle à la dématérialisation des actes juridiques tenant à une formalité exigée, en plus de la signature de celui qui s'engage, pour une catégorie d'actes sous seing privé.

En application l'article 1326 du code civil, tous les actes unilatéraux, c'est-à-dire les actes par lesquels une personne s'oblige envers une autre sans réciprocité (reconnaissance de dettes, cautionnement, …), doivent comporter la mention manuscrite, en lettres et en chiffres, de la somme d'argent ou de la quantité de biens promise. A défaut de cette mention, l'acte perd de sa force probante et ne peut valoir que comme commencement de preuve par écrit laissé à l'appréciation du juge.

A l'origine, cette disposition était destinée à protéger le débiteur contre une fraude du créancier mais elle est aussi un moyen d'attirer son attention sur la portée de son engagement. Il n'est donc pas souhaitable de supprimer cette règle de preuve, mais il y a lieu, en revanche, de l'aménager, l'intéressé pouvant écrire les mentions requises par la loi aussi bien au moyen d'un stylo que d'un clavier d'ordinateur.

Ainsi en substituant aux mots « de sa main » les mots « par lui-même », le présent article rend la formalité imposée par l'article 1326 du code civil compatible avec un environnement électronique.

La Commission a *adopté* 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, dans la collectivité territoriale de Mayotte et dans les territoires d'outre-mer.

Les deux assemblées parlementaires ayant adopté en termes identiques le projet de loi constitutionnelle modifiant le statut de la Polynésie française qui, sous réserve de l'accord du Congrès, deviendra un pays

d'outre mer, le Sénat a remplacé la référence aux territoires d'outre-mer par la mention de la Polynésie française et de Wallis et Futuna.

La Commission a *adopté* l'article 5 sans modification.

*
* *

La Commission a adopté l'ensemble du projet sans modification.

*
* *

En conséquence, la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République vous demande d'adopter sans modification le projet de loi (n° 2158), adopté par le Sénat, portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique.

TABLEAU COMPARATIF

___

Texte en vigueur	Texte du projet de loi	Texte adopté par le Sénat en première lecture	Propositions de la Commission
___	___	___	___
Code civil	Article 1er	Article 1er	Article 1er
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.	I. — L'article 1316 du code civil devient l'article 1315-1.	I. — L'article 1316 du code civil devient l'article 1315-1.	*(Sans modification).*
Chapitre VI De la preuve des obligations et de celle du paiement *Section I De la preuve littérale* § 1 Du titre authentique § 2 De l'acte sous seing privé § 3 Des tailles § 4 Des copies des titres § 5 Des actes récognitifs et confirmatifs	II. — Les paragraphes 1er, 2, 3, 4 et 5 de la section première du chapire VI du titre troisième du livre troisième du code civil deviennent respectivement les paragraphes 2, 3, 4, 5 et 6.	II. — Les paragraphes 1er, 2, 3, 4 et 5 de la section I du chapire VI du titre III du livre III du code civil deviennent respectivement les paragraphes 2, 3, 4, 5 et 6.	
	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 :	III. — Il est inséré, avant le paragraphe 2 de la section I du chapitre VI du titre III du livre III du code civil, un paragraphe 1er intitulé : « Dispositions générales », comprenant les articles 1316 à 1316-2 ainsi rédigés :	
	« *Art. 1316.* — 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 soient leur support et leurs modalités de	« *Art. 1316.* — 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	

Texte en vigueur	Texte du projet de loi	Texte adopté par le Sénat en première lecture	Propositions de la Commission
___	___	___	___
	transmission. « *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. « *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 déterminant par tous moyens le titre le plus vraisemblable quel qu'en soit le support ».	transmission. « *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. « *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 déterminant par tous moyens le titre le plus vraisemblable quel qu'en soit le support ».	
		Article 1er *bis (nouveau)*	Article 1er *bis*
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.		L'article 1317 du code civil est complété par un alinéa ainsi rédigé : « Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. »	*(Sans modification).*
	Article 2	Article 2	Article 2
	Après l'article 1322 du code civil, il est inséré un article 1322-1 ainsi rédigé : « *Art. 1322-1.* — La même force probante est	Après l'article 1316-2 du code civil, il est inséré un article 1316-3 ainsi rédigé : « *Art. 1316-3.* — L'écrit sur support électronique a la	*(Sans modification).*

Texte en vigueur	Texte du projet de loi	Texte adopté par le Sénat en première lecture	Propositions de la Commission
___	___	___	___
	attachée à l'écrit sous forme électronique lorsqu'il constate des droits et obligations et qu'il est signé. »	même force probante que l'écrit sur support papier. »	
	Article 3	Article 3	Article 3
	Après l'article 1322-1 du code civil, il est inséré un article 1322-2 ainsi rédigé :	Après l'article 1316-3 du code civil, il est inséré un article 1316-4 ainsi rédigé :	*(Sans modification).*
	« *Art. 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.	« *Art. 1316-4.* — 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.	
	« 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. »	« 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. »	
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			

Texte en vigueur	Texte du projet de loi	Texte adopté par le Sénat en première lecture	Propositions de la Commission
___	___	___	___
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.	Article 4 A l'article 1326 du code civil, les mots : « de sa main » sont remplacés par les mots : « par lui-même ».	Article 4 A l'article 1326 du code civil, les mots : « de sa main » sont remplacés par les mots : « par lui-même ».	Article 4 *(Sans modification).*
	Article 5 La présente loi est applicable en Nouvelle-Calédonie, dans les territoires d'outre-mer et dans la collectivité territoriale de Mayotte.	Article 5 La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans la collectivité territoriale de Mayotte.	Article 5 *(Sans modification).*

A N N E X E S

- **ANNEXE 1 :** Etude d'impact jointe au projet de loi relatif à l'adaptation du droit de la preuve aux nouvelles technologies et à la signature électronique.

- **ANNEXE 2 :** Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

- **ANNEXE 3 :** Fiche technique sur la signature électronique**.**

- **ANNEXE 4 :** Fiche technique sur la cryptologie.

ANNEXE 1

Projet de loi
relatif à l'adaptation du droit de la preuve
aux nouvelles technologies et à la signature électronique

Etude d'impact

ANNEXE 3 [1]

FICHE TECHNIQUE
SUR LA SIGNATURE ELECTRONIQUE

1. Le développement du commerce électronique s'accompagne d'une dématérialisation des échanges, des documents, des actes de commerce, *etc*.

Définir des moyens d'authentifier ces documents et ces échanges, sur le modèle du commerce traditionnel, par des moyens de signature appropriés apparaît donc nécessaire.

La directive européenne sur la signature électronique différencie nettement la signature électronique, qui est un terme générique, de la signature numérique, qui est une technique de signature parmi d'autres.

a) Signature électronique

La signature électronique est définie comme l'ensemble des procédés utilisant des technologies électroniques, qui permettent d'identifier de manière non ambiguë un signataire et d'authentifier les documents et actes qu'il a signés.

Elle se caractérise par sa capacité à établir un lien non ambigu entre l'identité du signataire (une personne physique, morale, une entité) et la signature : elle doit donc permettre d'authentifier le signataire. Ce lien ne doit résulter que de la seule volonté du signataire et la technologie utilisée doit permettre de vérifier si la signature a été modifiée, altérée ou falsifiée.

b) Signature numérique

La signature numérique est une forme de la signature électronique utilisant des algorithmes à clés asymétriques.

Une signature numérique est un morceau de code qui est envoyé avec un message (un document) dans l'unique but d'identifier l'émetteur et de vérifier que le message ou document est resté intègre (n'a pas été modifié) pendant le transport. On utilise là aussi une technique de clés asymétriques qui est actuellement la seule technique éprouvée et opérationnelle garantissant l'unicité de la signature et du signataire.

2. La signature électronique peut être utilisée par quelqu'un dans le but d'authentifier l'identité de la personne émettrice du message ou du signataire du document. Elle permet alors d'assurer que le contenu du message ou du document envoyé n'a pas été modifié. L'environnement de confiance, que permet la signature manuscrite, doit être transposé au monde d'Internet dont la signature électronique sera l'outil.

Les avantages de la signature électronique sont : la facilité d'envoi et l'impossibilité d'usurper l'identité d'une autre personne. Elle assure l'authentification (de

---

([1]) Annexe élaborée par l'Echangeur, Centre européen de réflexion et de formation pour le commerce du futur.

l'émetteur), l'intégrité (sur le contenu du message) et la non-répudiation (preuve de bonne foi, valeur juridique).

3. Différentes technologies sont possibles.

a) Certificateurs

Une signature numérique ne peut être reliée à une entité de façon non ambiguë que si un document certifié par une autorité de confiance atteste du lien entre la clé publique de l'entité et son identité.

Une authentification nécessite donc la présentation d'un certificat.

Un certificat numérique établit un lien entre l'identité d'un individu, d'une organisation, d'une entité et une paire de clés électroniques servant à crypter, décrypter et signer des informations numériques.

Certificat à clé publique

Dans ce cas, le certificat établit un lien entre l'identité de l'individu et sa clé publique. Ce lien est certifié par une autorité de certification.

En simplifiant, le certificat numérique joue, sur l'Internet ou l'intranet, le même rôle que la carte d'identité, le passeport ou le badge magnétique d'accès : il garantit l'identité du porteur et si l'on utilise des certificats à clé publique, on peut signer et coder un document.

Un certificat numérique établit un lien entre une clé publique et une entité, une organisation, un individu. Le lien doit être attesté par une autorité tierce digne de confiance appelée l'autorité de certification.

Les certificats numériques standards recourent à la cryptographie à clé publique qui associe dans son principe une paire de clés, l'une rendue publique, l'autre gardée strictement secrète appelée clé privée.

La clé privée sert à créer des signatures électroniques. C'est pourquoi elle doit être gardée secrète par son utilisateur.

La clé publique, elle, est largement diffusée dans des répertoires électroniques accessibles en ligne et sert à vérifier la signature numérique.

Pour vérifier une signature, il faut connaître l'identité du signataire du message.

L'association d'une paire de clés publique et privée n'établit pas de lien direct non ambigu avec une entité : c'est seulement un lien entre deux clés numériques. C'est le certificat qui atteste du lien entre la clé publique et l'identité de l'entité ; il permet de vérifier si la clé correspond à la bonne identité.

Généralement, un certificat a la forme suivante :

nom ou pseudonyme du signataire
clé publique du signataire
type de clé
sa position dans l'entité ou l'organisation
cas de résiliation, répudiation
référence à des documents officiels l'identifiant
limitations des responsabilités
nom du certificateur
algorithme utilisé
sa profession
assurances
date d'émission du certificat
les informations visées par le certificat

Autorité de certification (Certplus, filiale française de Verisign, Globalsign en Belgique, …)

Une autorité de certification authentifie le lien entre l'identité d'une organisation d'un individu et sa clé publique. Elle prend en charge la délivrance et souvent la gestion des certificats numériques.

Dans les faits, une autorité de certification signe le certificat avec sa clé privée (pour cela, il suffit d'un logiciel spécialisé) et fait office d'autorité d'enregistrement des clés publiques des entités qui se sont ainsi fait certifier.

Autorité d'enregistrement (experts comptables, commissaires aux comptes, chambre de commerce, …)

Organisme, responsable de l'identification et de l'authentification d'entités qui demandent un certificat mais qui n'est ni l'autorité de certification ni l'autorité d'attribut.

L'autorité d'enregistrement ne signe pas de certificat mais examine les pièces justificatives de l'entité demandant le certificat.

Elle ne donne l'ordre de certification à l'autorité de certification que si elle juge que les pièces justificatives correspondent à l'usage qui va être fait du certificat (conformité à l'usage).

Délivrance des certificats

Dans le cas le plus simple, le fonctionnement est le suivant.

La personne souhaitant obtenir un certificat auprès d'une autorité de certification pour pouvoir attester du lien entre son identité et une clé publique devra générer une paire de clé publique/privée et envoyer la clé publique et des pièces prouvant son identité à une autorité de certification.

L'autorité de certification vérifie le lien entre l'identité de l'entité et la clé publique par des moyens appropriés plus ou moins rigoureux (c'est ce qui définira le niveau de sécurité du certificat). Si la vérification s'avère positive, l'autorité crée un certificat attestant du lien entre son identité et la clé publique générée, certificat qui pourra être présenté à un tiers pour authentification ou dans le cadre de la signature électronique.

L'entité A utilise un algorithme de *hash* pour calculer le *digest* (résumé) de son message puis code le *digest* et le message avec sa clé privée. Il envoie le message et le *digest* codés (KR) au destinataire B . S'il souhaite que le message reste confidentiel, il peut coder le message et le *digest* avec la clé publique de B avant de l'envoyer à B.

A la réception du message, B décode le message avec sa clé privée ce qui lui permet de prendre connaissance du contenu du message, puis il vérifie la signature de la façon suivante :

— il se procure la clé publique de A pour décrypter le message et le *digest*, ce qui lui donne une forte certitude quant à la provenance du message signé : c'est celle de A ;

— il n'a plus qu'à s'assurer que la signature n'a pas été modifiée. Il se procure l'algorithme de *hash* utilisé, qui est public, et calcule le *digest* du message qu'il a reçu puis le compare au *digest* dont il a pu prendre connaissance en décodant « KR » avec la clé publique de A.

Si les deux résumés sont identiques, c'est que la signature n'a pas été modifiée.

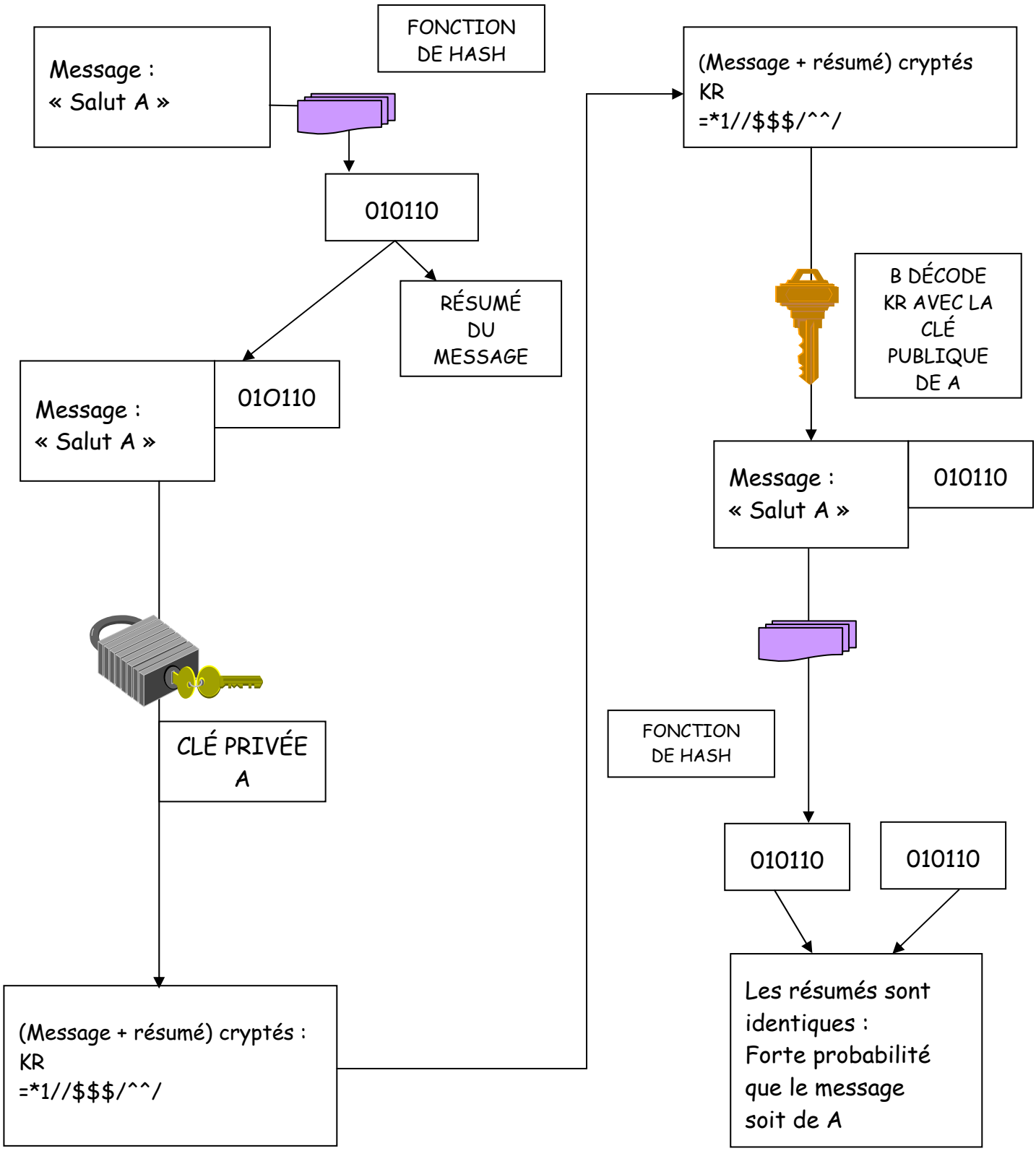
Le message provenant de A et la signature n'étant pas modifiés, il y a une forte probabilité que le message soit bien signé par A.

Le hachage

Cet outil est utilisé pour assurer l'intégrité des données, lorsque l'on communique avec une autre partie et que l'on veut s'assurer que les données et le message n'ont pas été changés.

Une fonction de hachage transforme un message de taille variable en un résumé de taille fixe qui est l'image cryptée unique du message d'origine, aucun autre message ne peut aboutir au même résumé (*digest*). Cela signifie que si quelqu'un change le message d'origine, le résumé ne sera pas le même et l'on s'apercevra de l'altération du message.

En pratique, on communique le « résumé » du message sur un canal parallèle en mode sécurité au destinataire ce qui lui permettra de comparer les deux résumés lors de la réception du message et ainsi de s'assurer de son intégrité. Le résumé (*digest*) du message est crypté en même temps que le message d'origine et communiqué au destinataire.


Message :
« Salut A »
FONCTION
DE HASH
010110
RÉSUMÉ
DU
MESSAGE
Message :
« Salut A »
010110
CLÉ PRIVÉE
A
(Message + résumé) cryptés :
KR
=*1//$$$/^^/
(Message + résumé) cryptés
KR
=*1//$$$/^^/
B DÉCODE
KR AVEC LA
CLÉ
PUBLIQUE
DE A
Message :
« Salut A »
010110
FONCTION
DE HASH
010110
010110
Les résumés sont
identiques :
Forte probabilité
que le message
soit de A

b) Carte à puce

Il est envisageable d'avoir sa signature électronique sur une carte à puce juste après son inscription auprès d'une autorité de certification. Il suffira par la suite d'insérer sa carte dans un lecteur connecté à un ordinateur. Pour apposer sa signature électronique, l'utilisateur rentrera alors son code PIN.

Cette technologie offre plus de sécurité car la signature se trouve sur la puce et non plus sur un ordinateur et plus de souplesse car un ordinateur muni du lecteur de carte pourra accueillir plusieurs utilisateurs, qui devront insérer leur carte personnelle.

c) Biométrie

La solution biométrique permet d'identifier les personnes à partir de leur visage. C'est une solution qui mesure des paramètres physiques, par opposition à des solutions comme la reconnaissance de la signature qui mesurent des paramètres comportementaux.

La biométrie présente des avantages par rapport aux cartes à puces avec code PIN : on peut l'oublier, se le faire voler,…

Le matériel requis est variable. Il dépend de l'utilisation que l'on veut faire de cette solution. Le matériel minimum requis est : une caméra quelle qu'elle soit ; un PC ; un logiciel permettant de comparer les images capturées avec les modèles constituants la base de données.

Pour utiliser une solution de biométrie, il est toujours nécessaire de rentrer dans un premier temps un modèle (ou plusieurs) des paramètres mesurés dans la base de données. Le système prend alors au moins deux photos du visage sous des angles différents afin de pouvoir faire la différence entre une photo et le vrai visage (reconstitution 3D).

On demande un identifiant. Cela sert à limiter le nombre de comparaisons à faire. En effet, le système n'a pas à reconnaître une personne parmi tous les modèles de la base de données mais simplement à comparer l'image à celle de l'identifiant.

Il est beaucoup plus rapide de coupler les solutions de biométrie à des identifiants lorsque les bases de données sont grandes (clientèle d'une banque). C'est également beaucoup plus fiable.

Cette technologie peut donner lieu à différentes applications :

– Contrôle d'accès à un PC ; contrôle d'accès à un réseau et contrôle d'accès à certaines données ; applications pour les services financiers : sécurisation des consultations de comptes sur Internet ; sécurisation pour des transferts d'argent sur Internet ; sécurisation pour des accès aux back offices de banques ;

– Contrôle d'accès à des lieux.

Les autres possibilités offertes par cette technologie sont :

– La reconnaissance des empreintes digitales ; environ 5 % de gens n'a pas d'empreintes digitales suffisamment lisibles pour fonctionner avec les solutions traditionnelles.

– La reconnaissance biométrique de la voix, selon deux types de système : par téléphone ; avec un microphone.

Par ailleurs, ces systèmes peuvent être trompés par un enregistrement vocal si les mots à prononcer sont invariables. Il existe, par exemple, le système TrueFace dont les performances, selon les concepteurs, sont les suivantes :

– erreurs d'acceptation : faible
– erreurs de rejet : < 0,2 %
– facilité d'utilisation : excellente
– rapidité de l'identification : 1,5 seconde

ANNEXE 4 [2]

FICHE TECHNIQUE SUR LA CRYPTOLOGIE

1. La cryptographie symétrique

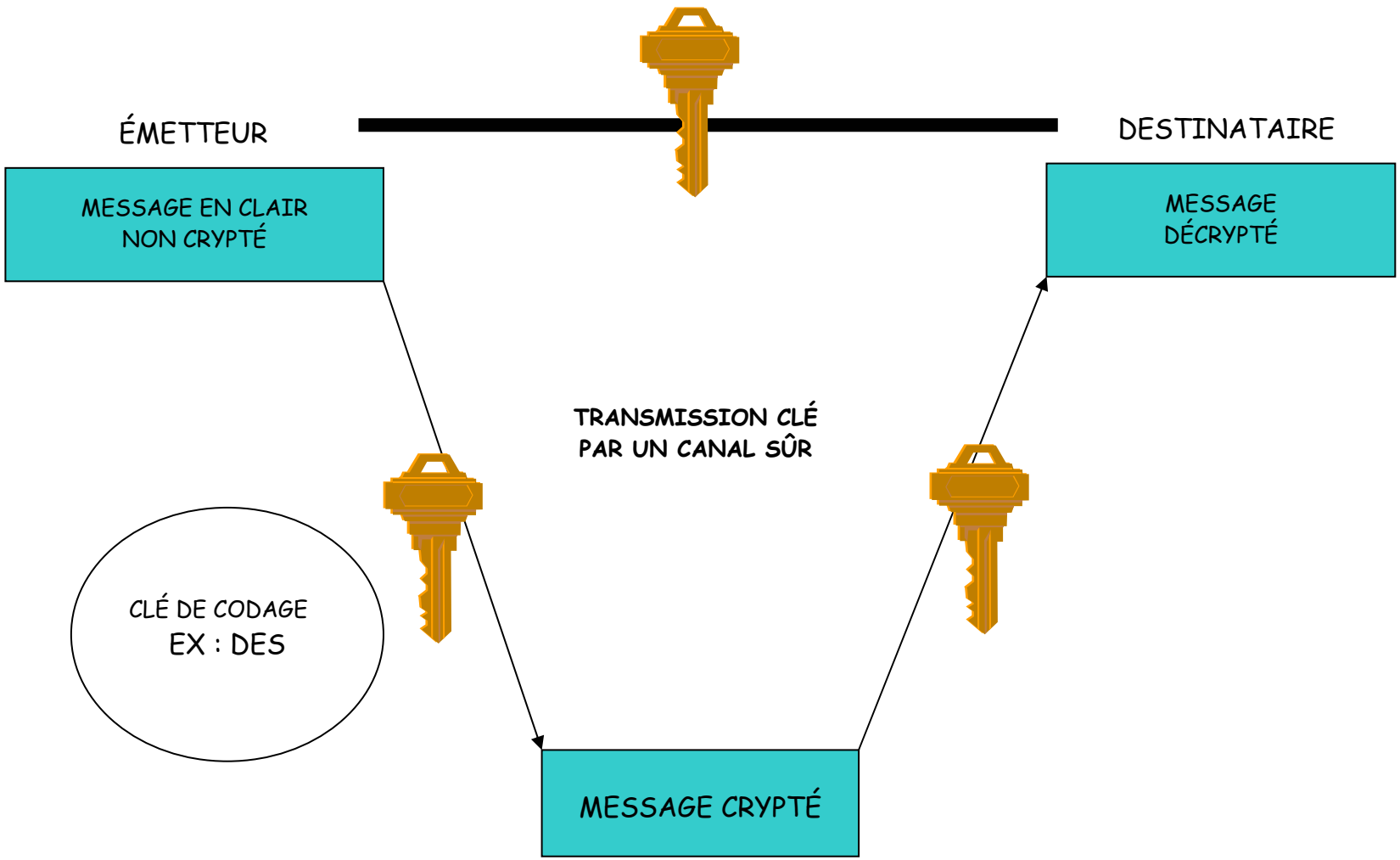
Les algorithmes symétriques sont aussi appelés algorithmes à clé privée. En effet, lorsque l'on crypte une information à l'aide d'un algorithme symétrique avec une clé secrète, le destinataire utilisera la même clé secrète pour décrypter. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée auparavant, par courrier, par téléphone ou lors d'un entretien privé.

La cryptographie à clés symétriques permet le chiffrement et le déchiffrement d'un message en utilisant la même clef. Cette technique fonctionne à partir d'algorithmes rapides et utilise des clés de taille réduite.

Au-delà de l'avantage de la rapidité, se pose le problème de la distribution des clés, qui doivent rester secrètes. Lors de la distribution, l'émetteur et le récepteur doivent partager la même clé. Il faut assurer la sécurité du mode de communication des clés. Cela pose problème en particulier sur les réseaux non sécurisés. Ce problème est augmenté par la combinatoire à gérer entre le nombre d'émetteurs et le nombre de récepteurs. En entreprise, ce système reste gérable. Par contre, si on travaille avec des applicatifs s'adressant à un grand nombre d'utilisateurs, le nombre de clés à gérer s'avère trop important.

([2]) Elaborée par l'Echangeur, Centre européen de réflexion et de formation pour le commerce du futur.

CONFIDENTIALITÉ : LA CRYPTOGRAPHIE SYMÉTRIQUE



2. La cryptographie asymétrique

Les algorithmes asymétriques sont aussi appelés algorithmes à clé publique. C'est à dire que pour crypter un message, l'émetteur utilise sa clé privée et le destinataire sera *a priori* le seul à pouvoir le décrypter à l'aide de la clé publique de l'émetteur, trouvée dans le répertoire du destinataire.

Chaque navigateur internet (Netscape communicator, Internet explorator,…) possède plusieurs clés publiques limitées selon la législation (56 bits). Aux Etats-Unis, il existe la possibilité de crypter à 126 bits : en installant la dernière version de son navigateur internet ; ou en téléchargeant le dernier module de cryptage.

La législation française actuellement en vigueur pose les règles suivantes.

Pour la cryptologie « de chiffrement » :

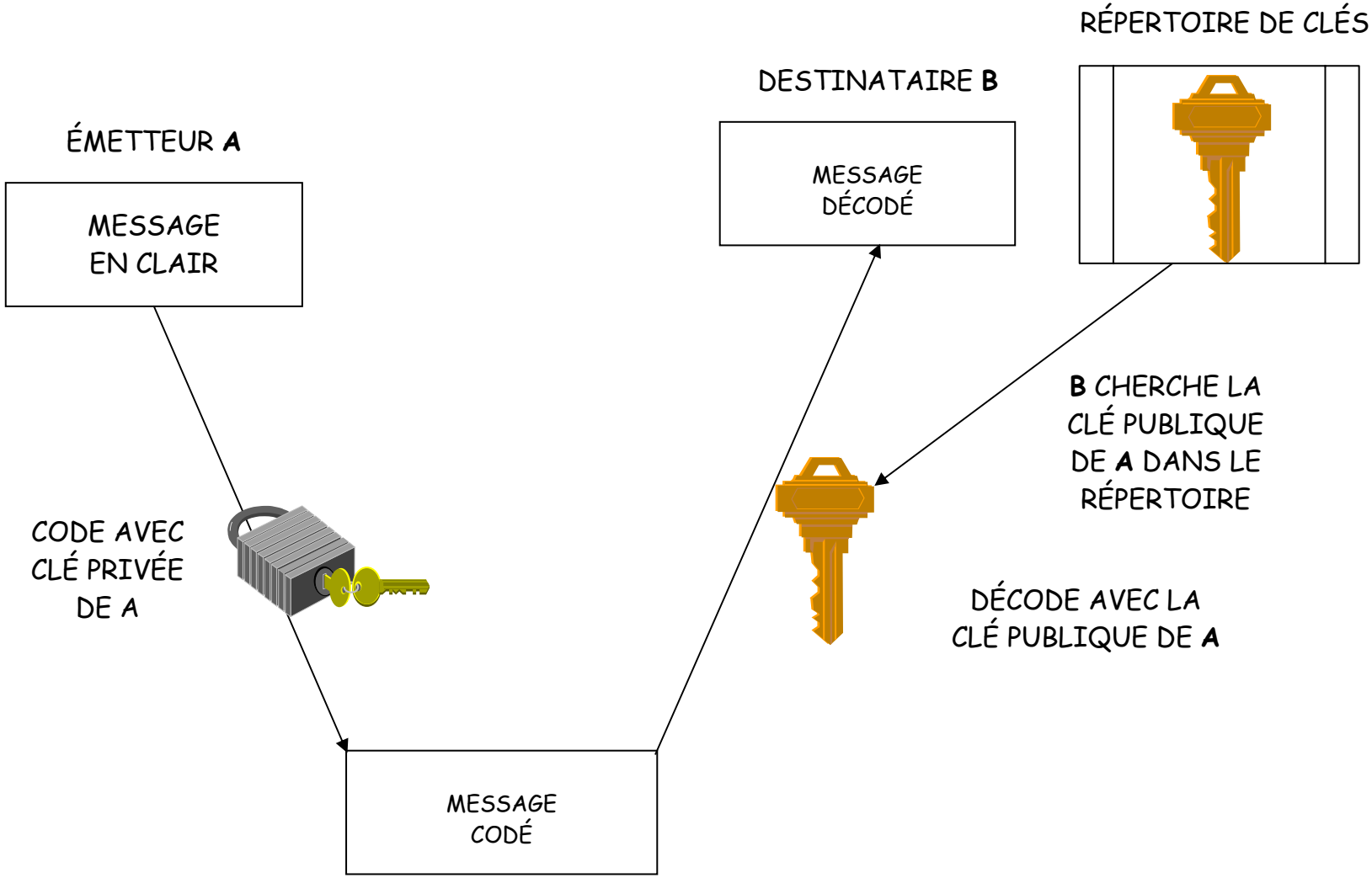
– jusqu'à 40 bits : utilisation libre, déclaration standard nécessaire pour la fourniture ;

– de 40 à 128 bits : l'usage est libre s'il s'agit d'une personne privée ou si la technologie a fait l'objet d'une déclaration, commercialisation après déclaration standard ;

– plus de 128 bits : commercialisation après autorisation préalable, utilisation libre si couverte par l'autorisation du fournisseur ou si dépôt des clés chez un tiers de confiance.

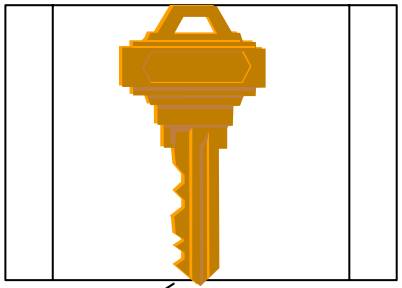
– *Pour la cryptologie « d'authentification »* : usage libre, commercialisation après déclaration simplifiée.

Authentification de l'émetteur



Authentification du destinataire

RÉPERTOIRE DE CLÉ



ÉMETTEUR A

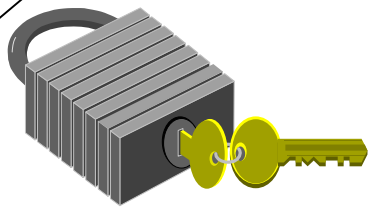
MESSAGE
EN CLAIR

A CHERCHE LA CLÉ PUBLIQUE DE B DANS LE RÉPERTOIRE

MESSAGE CODÉ

DESTINATAIRE B

MESSAGE DÉCODÉ



B DÉCODE LE MESSAGE AVEC SA CLÉ PRIVÉE

LISTE DES PERSONNES CONSULTÉES PAR LE RAPPORTEUR

1. Ont été reçus à l'Assemblée :

– *Chambre de commerce et d'industrie de Paris* : M. Jean-Paul SAILLARD, secrétaire général du groupe AXA ; Mme Dominique MORENO, chef du département du droit civil et commercial ;

– *Chancellerie* : M. Pierre-Eric SPITZ, conseiller technique ; Mme Catherine CHADELAT, sous-directrice de la législation civile ; M. Laurent JACQUES, magistrat au bureau du droit civil général ;

– *Conseil d'Etat* : Mme Isabelle FALQUE-PIERROTIN, maître des requêtes, rapporteuse générale de l'étude sur *Internet et les réseaux numériques* ;

– *Conseil supérieur du notariat* : M. Jean-Paul DECORPS, président ; M. Jean-Dominique MATHIAS, responsable du département de la réglementation de l'éthique notariale ;

– *Journaux officiels* : Mme de LA PRESLE, administratrice civile, chargée de mission ;

– *La Poste* : M. Jean-Bernard de CÉROU, directeur du développement des nouveaux services ; Mme Inès SEN, directrice de l'intelligence économique, Comité des nouvelles technologies ;

– *Mission pour le commerce électronique* : M. Francis LORENTZ, président ;

– *Société CERTPLUS* : M. Jacques PANTIN, président-directeur général.

2. Ont également communiqué leurs observations :

– l'Association française des banques ;

– l'Association française des établissements de crédit et des entreprises d'investissement (AFECEI) ;

– Mme Isabelle de LAMBERTERIE, directrice de recherche au CNRS, membres du groupe d'experts ayant réalisé une étude sur *L'écrit et les nouveaux moyens technologiques au regard du droit*, à la demande du GIP Droit et justice ;

– M. Thierry PIETTE-COUDOL, avocat à la Cour de Paris et le Groupe ad hoc signature électronique (GAC) lancé par IALTA France et EDIFRANCE ;

3. Déplacement à l'*Echangeur* (Centre européen de réflexion et de formation pour le commerce du futur)

Le rapporteur et plusieurs de ses collègues ont été reçus par Mme Cécile ALVERGNAT, membre de la Commission nationale de l'informatique et des libertés, directrice de L'*Echangeur*, pour une présentation des procédés rendant effective l'adaptation du droit de la preuve aux technologies de l'information : protocole SSL (socket secure layer) ; certificats ; signature électronique ; carte à puce ; biométrie.