Le Livre Blanc

de la signature électronique

Réalisé par le groupe de travail du Club CSA
présidé par :
Alain Bensoussan et Charles Copin
Assistés par :
Marion Depadt

Editeur : ANALYSES et SYNTHESES

Le Livre Blanc de la signature électronique

Novembre 1999

Remerciements à tous les membres du groupe de travail
pour leur participation à l'élaboration de ce livre blanc.

SOMMAIRE

Préface

C'est en mai 1999 que le Club CSA décida de lancer un groupe de travail sur le thème de la signature électronique. Les partenaires du Club ont répondu à l'appel,preuve de l'intérêt du sujet non seulement au niveau juridique mais aussi technique.

Et c'est bien là que réside l'originalité de ce groupe de travail : réunir dans un même lieu des spécialistes juridiques ou techniques impliqués quotidiennement dans leur rôle d'acteurs de la carte à puce. Ainsi, le groupe a été composé de représentants d'industriels, de sociétés de services, de réseaux de cartes bancaires et d'émetteurs de cartes,notamment dans le domaine de la santé.

C'est dire que les réflexions de ce groupe de travail ont permis de mettre en évidence non seulement les aspects juridiques de la signature électronique mais aussi les aspects techniques de mise en œuvre de la signature électronique.

Les techniciens ont appris le langage juridique enseigné de façon brillante par l'un des experts incontesté dans ce domaine : Maître Alain Bensoussan.Qu'il en soit ici remercié.

A l'heure où le sujet de la signature électronique fait l'objet de décisions parlementaires tant en France qu'à l'étranger, le souhait du groupe de travail est que les aspects techniques soient autant pris en compte que les aspects juridiques pour une bonne application des principes permettant à tout citoyen d'être sur un même pied d'égalité.

La carte à puce est un objet nomade possédé par la quasi-totalité de la population française,elle garantit la confidentialité et l'intégrité des informations sur son porteur, elle peut ainsi contenir précieusement les éléments fondamentaux pour la réalisation de la signature électronique.

Mon souhait est que les hommes de loi puissent tenir compte de cette réalité.

Charles Copin
Responsable du Club CSA
Directeur de Analyses & Synthèses

Généralités sur le groupe de travail

L'intérêt majeur du groupe de travail a été de réunir des experts, aussi bien dans le domaine juridique que technique, qui ont pu avoir des échanges concrets par rapport aux besoins tant techniques que juridiques en la matière et ont pu confronter le droit et la technique par une imprégnation mutuelle.

L'objectif principal du groupe de travail a été d'apporter une définition de l'état de l'art de la signature électronique en matière technique et juridique,notamment au regard des projets de réglementations tant françaises qu'européennes.

Limitations

Le présent Livre blanc ne se veut pas une étude exhaustive sur la signature électronique.

Notamment,il se limitera à une étude de la signature électronique dans le commerce électronique,envisagé dans son acceptation la plus large.

C'est,en effet,essentiellement en raison du développement croissant de ce dernier que la nécessité de s'interroger sur la signature électronique et de mettre en place un cadre législatif est apparue.

On ne peut en outre contester le fait que la reconnaissance de la signature électronique est un élément déterminant dans l'essor du commerce électronique.

Par ailleurs, les questions liées à la certification ne seront abordées que dans la mesure où elles seront nécessaires au suivi d'un raisonnement ou à une démonstration.

Enfin, sur un tout autre plan, hormis un certain nombre de références aux législations étrangères,le présent Livre blanc se limitera à une étude de la signature électronique en France.

Toutefois,ce Livre blanc ne correspond qu'à une première étape et le groupe de travail envisage d'étendre sa réflexion, dans un second temps, au niveau européen, voire international.

La signature électronique et le commerce électronique

Si la signature électronique ne se réduit pas au commerce électronique[1], commerce électronique et signature électronique sont en revanche intimement liés.

L'exposé des motifs du projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique fait d'ailleurs directement référence au lien existant entre ces deux " phénomènes " : *" (...) l'adaptation de notre droit de la preuve est devenue une nécessité.Elle permettra en effet à la France, à ses entreprises et à ses consommateurs, de profiter pleinement de l'essor du commerce électronique et contribuera de surcroît au renforcement de l'efficacité du système juridique français "*[2].

Le Livre blanc vise donc à appréhender les questions relatives à la signature électronique au regard du commerce électronique, ce terme étant compris dans son sens le plus large et non pas seulement dans ses aspects purement économiques.

La signature électronique en matière de santé,notamment,a vocation à être englobée dans l'étude menée dans le présent Livre blanc.

En revanche, le commerce électronique dans ses aspects réglementaires ne sera pas inclus dans le livre.

La nécessaire évolution textuelle

Une refonte des textes relatifs aux droits de la preuve avait à plusieurs reprises été requise,à l'exemple du Québec notamment ou encore de l'Allemagne.

Ainsi, le Conseil National du Crédit et du Titre en 1997 s'exprimait de la façon suivante :

- *" Ils [les autres membres du groupe] ont jugé souhaitable,*

1.A titre d'exemple :la signature électronique pourra être utilisée lors de votes, comme les votes aux assemblées générales, ou lors d'élections professionnelles

2.Projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique en date du 1er septembre 1999

pour des raisons tenant à la nature du phénomène de la dématérialisation, d'aller plus loin, en procédant par voie d'une modification de l'article 1348 : l'exception au principe de la preuve écrite serait ainsi admise de façon plus large.[3]".

En effet, dans le cadre de transactions entre des personnes " absentes " concernant des opérations dématérialisées,il est devenu nécessaire de sécuriser le consentement,aussi bien pour être sûr que celui-ci a bien été donné, que pour se préconstituer la preuve de celui-ci.

C'est à ces conditions seulement que les échanges électroniques pourront réellement se développer.

Les nouveaux textes

Plusieurs textes essentiels existent aujourd'hui. Ces projets servent de base à la réflexion sur la signature électronique,objet du présent Livre blanc.

3.Rapport du Conseil National du Crédit et du Titre sur les problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres, mars 1997, p.63

2.1 DE LA SIGNATURE A LA SIGNATURE ELECTRONIQUE

2.1.1 Les définitions

Avant de commencer l'étude des définitions de la signature et de la signature électronique, un rappel historique comparatif sur l'existence et le contenu des définitions doit être fait.

Il convient en effet de rappeler que la tradition romano-germanique est d'utiliser des termes non définis alors que la common law a toujours eu tendance à définir les termes utilisés.

Par ailleurs, même lorsque les termes sont définis, on peut être confronté à différents types de définitions.

Le premier type est la définition fermée, qui correspond généralement à la définition des techniciens.

Le deuxième type est la définition ouverte, et correspond plus généralement à la définition des juristes.

2.1.2 La signature dans les textes français

En France,la notion de signature n'est pas définie dans les textes.

Tenter de définir la signature fait apparaître deux aspects qu'il convient de distinguer :la fonction de la signature et la forme de la signature.

la fonction de la signature

La signature est,en principe,définie par rapport à ses fonctions.

Ainsi,dans son rapport sur " Internet et les réseaux numériques ", le Conseil d'Etat précise que *" constitue une signature un procédé qui permet de remplir avec efficacité certaines finalités : identification du signataire et manifestation de sa volonté d'adhérer au message signé qui est réputé intègre "*[1].

1.Rapport adopté par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998

De façon générale, on entend par signature le lien entre le sujet de droit et l'objet de droit, plus exactement le lien du sujet de droit vers l'objet de droit.

la forme de la signature

La signature est très souvent un signe écrit à la main, portant la mention du patronyme de la personne.

Une telle description semble évidente aujourd'hui.

Toutefois, la mention du patronyme dans la signature n'est pas une obligation.

On peut ainsi citer Monsieur Larrieu selon lequel *" (...) est jugée recevable la signature par apposition d'un " pseudonyme " si celui-ci constitue une marque caractéristique et personnelle.*

La mention du seul prénom peut suffire.

Cependant, il faut que l'identité du signataire soit certaine, donc on tiendra compte du genre et de la destination de l'écrit.

Il en va de même pour de simples initiales (...) "[1].

En ce qui concerne la possibilité d'utiliser un pseudonyme,signalons dès maintenant que cette possibilité perdure dans les nouveaux textes, dans la mesure où la position commune en vue de l'adoption de la directive prévoit que les Etats membres *" ne peuvent empêcher le prestataire de service de certification d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire "*[2].

La forme de la signature semble ne faire l'objet d'aucune précision dans les textes de portée générale.

Si la forme de la signature avait été définie dans le Code civil,elle aurait certainement été définie,à n'en pas douter, en liaison avec

---

1. J.Larrieu "Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ?" ; Cahier Lamy du droit de l'informatique, novembre 1988 (H) et décembre 1988 (I)

2. Position commune CE) N° 28/1999 arrêtée par le Conseil le 28 juin 1999 en vue de l'adoption de la directive 1999/.../CE du Parlement européen et du Conseil du ...sur un cadre communautaire pour les signatures électroniques, article 8, 3., JOCE du 27 août 1999

les moyens techniques utilisés à l'époque, et donc par rapport à un support papier.

L'absence de définition permet une interprétation large de la notion de signature.

C'est ainsi qu'a été reconnue par la jurisprudence la validité d'une sorte de "signature informatique"[1].

Rien ne s'oppose en effet à ce que la signature revête une forme autre qu'une signature sur support papier.

La position commune en vue de l'adoption de la directive et le projet de loi,s'ils sont adoptés, clarifieront néanmoins la situation dans la mesure où ils distinguent clairement la signature du support sur lequel elle est apposée.

2.1.3 Evolution des signatures

Les premières signatures connues ne sont pas des signatures manuscrites,mais d'autres formes de signature,telle que le sceau.

La signature manuscrite occupe toutefois une place prépondérante dans les différents types de signature depuis de nombreuses années.

La signature manuscrite peut être représentée comme l'association :

- d'un sujet de droit :celui qui s'engage ;

- d'un objet de droit :l'engagement ;

- d'un support de droit (papier, etc.).

La signature manuscrite présente quatre paramètres :

- elle est manuscrite ;
- elle est unique ;
- elle est simple ;
- elle ne dépend pas de l'acte.

1.CA Montpellier, 9 avril 1987, 1ère ch., société Crédicas SA / Yves J., JCP, éd. G, 1988, II, 20984

Il faut par ailleurs faire remarquer dès maintenant que malgré les diverses évolutions ayant affecté la signature manuscrite, et notamment le support de celle-ci, ne serait-ce qu'avec le développement de la reprographie, la signature manuscrite présente toujours la même force probante et la même portée.

D'autres types de signatures sont ensuite apparus. C'est, par exemple,le cas de la signature par griffe,utilisée particulièrement dans le milieu bancaire.

Toutefois il ne semble pas que les nouveaux types de signature aient eu une portée aussi large que la signature manuscrite ...jusqu'à l'apparition de la signature électronique.

Mais de quand date l'apparition de ce nouveau type de signature ?

Répondre à cette question nécessiterait de répondre de façon préalable à la question suivante :que recouvre le terme de signature électronique ?

Faut-il l'entendre au sens large ou étroit ?

Ainsi, les différents types de signature tels que le double-clic ou l'utilisation d'une carte bancaire peuvent-ils recevoir la qualification de signature électronique ?

On peut,par ailleurs,se demander pourquoi avoir retenu le terme " électronique " pour désigner les nouveaux types de signature et non, par exemple, le terme de signature " numérique " ou tout simplement de signature " informatique ", ainsi que ce terme est employé par la Cour d'appel de Montpellier précité.

Il semble toutefois qu'aujourd'hui le terme de signature électronique soit acquis tout comme celui de commerce électronique.

C'est en outre ce terme qui a été retenu d'ores et déjà dans un certain nombre de textes.

Ainsi,l'arrêté du 9 avril 1998 relatif aux spécifications physiques et logiques de la carte de professionnel de santé précise que " *des données techniques inscrites dans le composant électronique de cette carte à microprocesseur assurent la sécurité et la protection des données, les fonctions de signature électronique (...)* "[1] .

1. Article 3 de l'arrêté du 9 avril 1998,JO du 16 avril 1998 page 5851

De même, les différents projets de textes, tant communautaires que français, retiennent ce terme.

Cette multiplicité de signatures que pourrait recouvrir le terme de signature électronique amène d'ores et déjà à se poser une question :y a-t'il une ou plusieurs signatures électroniques ?

2.2 LA SIGNATURE ELECTRONIQUE DANS LES NOUVEAUX TEXTES

Les projets de texte marquent principalement la reconnaissance de la validité de la signature électronique.

2.2.1 La position commune en vue de l'adoption de la directive [1]

Dans sa communication au Parlement européen du 13 mai 1998 présentant la première proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, la Commission rappelait que *" la vérification de l'authenticité et de l'intégrité des données ne prouve pas nécessairement l'identité du signataire qui a généré les signatures électroniques. Comment le destinataire peut-il, par exemple, savoir si l'expéditeur est réellement la personne qu'il prétend être ? (...) Cette information peut être fournie par le signataire en personne, en fournissant au destinataire une preuve satisfaisante.Un autre moyen consiste à recevoir confirmation par une tierce partie (...), ces tierces parties sont appelées " prestataires de services d'identification "* [2].

Dans son article premier, la proposition de directive issue de la

1. Position commune CE) N° 28/1999 arrêtée par le Conseil le 28 juin 1999 en vue de l'adoption de la directive 1999/.../CE du Parlement européen et du Conseil du ...sur un cadre communautaire pour les signatures électroniques, JOCE du 27 août 1999.

2.Communication de la Commission au Parlement européen,au Conseil,au Comité économique et social et au Comité des régions,com.(98) 297 final, 13 mai 1998.

position commune arrêtée par le Conseil le 28 juin 1999 précise, d'une part,qu'elle concerne l'utilisation et la reconnaissance juridique des signatures électroniques et,d'autre part,qu'elle institue un cadre juridique pour certains services de certification.

2.2.1.1 L'utilisation de la signature électronique

Dans son neuvième considérant, la proposition de directive du mois de juin 1998 limitait son champ d'application aux réseaux ouverts, position sur laquelle le Comité économique et social[1] s'était interrogé,souhaitant l'extension de la portée de la directive aux systèmes fermés,ouverts au public.

La position commune en vue de l'adoption de la directive précise *" qu'il y a lieu, néanmoins, de reconnaître juridiquement les signatures électroniques répondant aux exigences énoncées dans la présente directive et utilisées au sein de groupes fermés d'utilisateurs "* [2].

2.2.1.2 La définition de la signature

Le projet de texte de directive définit la signature électronique et crée une dualité.

Une distinction est en effet faite dans la nouvelle version du projet entre " signature électronique " et " signature électronique avancée ".

La définition de ces deux types de signature électronique,donnée par la position commune,est la suivante :

" Aux fins de la présente directive, on entend par :

1) " signature électronique ", une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ;

2) " signature électronique avancée ", une signature électro-

---

1. Avis du Comité économique et social sur la " Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques " adopté lors de la session des 2 et 3 décembre 1998

2. Position commune CE) N° 28/1999, précitée, considérant n° 16

nique qui satisfait aux exigences suivantes :

a) être liée uniquement au signataire ;

b) permettre d'identifier le signataire ;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif

et

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable " [1].

L'exposé des motifs du Conseil précise par ailleurs que la signature électronique avancée doit *" reposer sur un certificat agréé établi et délivré dans le respect d'un certain nombre d'exigences " et " être créée par un dispositif sécurisé de création de signature électronique ".*

Enfin,le point c) de la définition donnée par la directive amène à se poser la question suivante :à partir du moment où les moyens de création de la signature électronique doivent pouvoir être gardés sous le contrôle exclusif du signataire, faut-il en déduire que la mise en place d'un mandat dans le cadre de la signature électronique est exclu ?

Il semble toutefois que la définition du " signataire " issue de la position commune apporte une réponse à cette question dans la mesure où est signataire *" toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou personne physique ou morale qu'elle représente "* [2].

2.2.1.3 La reconnaissance juridique de la signature électronique

La position commune en vue de l'adoption de la directive se prononce, par ailleurs, sur les effets juridiques de la signature électronique d'une part et sur les effets juridiques de la signature

1. Position commune CE) N° 28/1999, précitée, article 2

2. Position commune CE) N° 28/1999, précitée, article 2, 3)

électronique avancée basée sur un certificat qualifié [1] et créée par un dispositif sécurisé de création de signature [2] d'autre part.

La lecture de l'exposé des motifs du Conseil semble permettre de dire que cette signature électronique avancée basée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature correspond en fait à la signature électronique avancée définie à l'article 2 de la position commune.

En ce qui concerne la signature électronique avancée, le texte prévoit que la signature électronique avancée basée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature non seulement doit être recevable comme preuve en *justice, mais également doit répondre " aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier "* [3].

En ce qui concerne la signature électronique " simple ", le texte dispose que :

" 2.Les Etats membres veillent 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

ou

- qu'elle ne repose pas sur un certificat qualifié

ou

- qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification

ou

- qu'elle n'est pas créée par un dispositif sécurisé de création de signature " [4].

1.Défini à l'article 2, 10) de la Position commune CE) N° 28/1999, précitée

2.Défini à l'article 2, 6) de la Position commune CE) N° 28/1999, précitée

3. Position commune CE) N° 28/1999, précitée, article 5, 1

4. Position commune CE) N° 28/1999, précitée, article 5, 2

2.2.1.4 La création d'un métier autour de la signature électronique

Les certificats qualifiés sont définis comme une *" un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II* [1]*"*.

Le prestataire de service de certification est, quant à lui, défini comme " toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques "[2] .

2.2.2 Le projet de loi [3]

2.2.2.1 Présentation générale

Avant d'examiner précisément dans quels termes le projet de loi aborde la question de la signature électronique, il convient de faire un certain nombre de remarques d'ordre général sur ce projet.

Tout d'abord, le projet ne porte pas uniquement sur la signature électronique.

Son objectif est plus vaste, visant à actualiser le droit de la preuve.

Il est ainsi l'occasion de définir la preuve par écrit dans la mesure où l'écrit,pas plus que la signature,ne fait l'objet d'une définition dans le Code civil.

Il a également pour objet de valider les conventions sur la preuve et de reconnaître la valeur juridique du document et de la signature électroniques.

1.Défini à l'article 2,5) de la Position commune CE) N° 28/1999,précitée

2. Position commune CE) N° 28/1999,précitée,article 2,11)

3.Projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique en date du 1er septembre 1999

2.2.2.2 Le contenu du projet de loi

Le nouvel article 1316 du Code civil, tel qu'il résulte de l'article 1er, III du projet de loi définit des termes utilisés depuis longtemps,ce texte définit la preuve littérale ou par écrit,de la façon suivante :

- *" 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 qu'elles que soient leur support et leurs modalités de transmission ".*

Cet article sépare donc l'écrit du support.Si le support de l'écrit peut ainsi,bien entendu,être un support papier, il peut tout aussi bien être, par exemple, électronique, magnétique, voire même oral.

Ce premier texte permet en fait d'introduire le concept général d'écrit avant d'aborder plus spécifiquement la notion d'écrit électronique,objet de l'article 1316-1 qui énonce que :

- *" 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 ".*

Sur la notion d'écrit " électronique ", il faut rappeler que trois mots au minimum " rivalisent " avec le terme " électronique ".

Il s'agit des mots : télécommunication - informatique - numérique.

Remarquons à ce sujet qu'il semble que les termes d'écrit manuscrit et électronique recouvrent l'ensemble des écrits existant aujourd'hui.

L'article 1316-1 exige que la personne dont émane l'écrit électronique " puisse être identifiée ", et non plus " soit identifiée " comme le prévoyait le précédent projet de loi.

Mais l'intérêt majeur de cet article se situe certainement dans la première partie de cette disposition qui accorde une force probante à l'écrit électronique identique à celle de l'écrit sur support papier.

Après l'article 1316-2 du Code Civil tel qu'il résulte du projet de loi,et qui pose un certain nombre de règles en matière de conflits de preuve, le nouvel article 1322-1 revient sur la force probante de la signature électronique ou, plus exactement, de l'écrit électronique en disposant que :

- *" La même force probante est attachée à l'écrit sous forme électronique lorsqu'il constate des droits et obligations et qu'il est signé. "*

Ces nouvelles dispositions qui entrent dans le cadre des développements du Code Civil consacrés à l'acte sous seing privé sont complétées par un nouvel article 1322-2, essentiel dans le devenir de la signature électronique :

- *" 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.*

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. "

Il faut entendre la " perfection " comme le mécanisme permettant au document de produire toutes ses conséquences de droit.

Quant au terme d'acte sous seing privé, rappelons qu'un tel acte correspond à un acte créateur de droit,opposable à la personne.

2.2.3 Les autres textes

2.2.3.1 La proposition de loi

Il peut être intéressant également de rappeler brièvement le contenu de la proposition de loi en date du 3 mars 1999 présentée par les sénateurs[1], dont certains éléments ont été repris dans la rédaction du projet de loi révisé.

[1] Proposition de loi visant à reconnaître la valeur probatoire d'un message électronique et de sa signature

Dans l'exposé des motifs, les sénateurs faisaient valoir que *" la signature électronique doit comporter les mêmes garanties que la signature manuscrite (...).Le Conseil d'Etat recommande de façon fort sage et opportune que la signature et le message électroniques constituent la preuve d'une transaction en cas de contestation (...).Il convient comme le propose le Conseil d'Etat de " reconnaître dans le code civil la valeur probatoire d'un message électronique répondant à deux exigences : l'authentification par une signature électronique fiable et la conservation du message sous le contrôle du signataire " "*.

Ensuite, le texte proposait que le Code Civil soit complété de la façon suivante :

- *" Un message électronique possède une valeur probatoire sous réserve du respect de deux conditions cumulatives :d'une part, que soit possible l'authentification par une signature électronique fiable, d'autre part, que soit assurée la conservation durable du message sous le contrôle du signataire "*[1].

Le projet de loi a pris en compte les remarques de la proposition de loi visant à conférer à l'écrit électronique une valeur probatoire équivalente à l'écrit manuscrit.

En effet,alors que le projet de loi en date du 29 octobre 1998 disposait :

- *" Il ne peut être prouvé par écrit électronique contre et outre un écrit rédigé sur des registres ou papiers quelconques et signé par les parties "* [2], refusant ainsi à l'écrit électronique la même valeur probatoire que l'écrit manuscrit, le nouveau projet de loi accorde,sous certaines conditions,à l'écrit électronique,la même force probante qu'à l'écrit manuscrit.

2.2.3.2 Les textes sur la santé

Les récents textes sur la santé font également partie des rares textes à aborder le problème de la signature électronique.

Deux des textes sur la santé traitent directement de la question de la signature électronique et de sa portée.

1.Article 1334 du Code Civil tel que résultant de la proposition de loi du 3 mars 1999

2.Article 1316-1 du Code Civil tel que résultant du projet de loi du 29 octobre 1998

Tout d'abord,le décret du 9 avril 1998 dispose que :

- *" Art. R. 161-58 - Pour les applications télématiques et informatiques du secteur de la santé, la signature électronique produite par la carte de professionnel de santé est reconnue par les administrations de l'Etat et les organismes de sécurité sociale comme garantissant l'identité et la qualité du titulaire de la carte ainsi que l'intégrité du document signé.Ainsi signés, les documents électroniques mentionnés à l'article L.161-33 sont opposables à leur signataire "*[1].

Par ailleurs, l'arrêté du 9 avril 1998 concernant les spécifications physiques et logiques de la carte de professionnel de santé précise que

- *" Des données techniques inscrites dans le composant électronique de cette carte à microprocesseur assurent la sécurité et la protection des données, les fonctions de signature électronique, d'authentification de la carte par un tiers et de participation au chiffrement des messages échangés.*

Ces données techniques sont les suivantes :

a)L'algorithme asymétrique "RSA" et les clés propres à la carte qui lui sont associées (...) ;

b) L'algorithme symétrique "A3S" et les clés propres à la carte qui lui sont associées (...) ;

c) L'algorithme "Diffie-Hellman" utilisé pour la mise en œuvre du service de confidentialité (...) " [2].

1. Article 2 du décret n°98-271 du 9 avril 1998 relatif à la carte de professionnel de santé et modifiant le code de la sécurité sociale et le code de la santé publique,JO du 12 avril 1998,pages 5714 et 5715

2. Arrêté du 9 avril 1998 relatif aux spécifications physiques et logiques de la carte de professionnel de santé,JO du 16 avril 1998,page 5851

De façon très générale, et depuis son apparition, la signature a pour vocation de faire le lien entre un objet et un sujet de droit.C'est encore le cas.

Plus précisément, les fonctions principales de la signature sont d'assurer l'identification (et/ou l'authentification) et la manifestation de l'adhésion de celui qui l'appose sur le document.

Et si la signature évolue,les fonctions de la signature restent quasi identiques.
En effet,si les contrats se forment aujourd'hui entre " absents ",il est toujours nécessaire d'être sûr de l'identité du cocontractant (authentification), du fait que c'est bien ce cocontractant qui s'engage (identification), que le cocontractant a donné son consentement sur le document tel qu'il est reçu par le récepteur (intégrité) et qu'il ne pourra pas revenir sur l'engagement qu'il aura ainsi pris (non-répudiation).

3.1 LA SIGNATURE ELECTRONIQUE, MOYEN D'AUTHENTIFICATION ET/OU D'IDENTIFICATION ?

3.1.1 Authentification et identification

Ces deux termes, dans le langage courant, peuvent désigner une même réalité et être employés indifféremment pour désigner une action :apporter la certitude de l'identité d'un individu.

Le Robert [1] donne les définitions suivantes :

- Authentification : *" action d'authentifier "* ;

- Authentifier : *" rendre authentique " ; " reconnaître comme authentique " ;*

- Authentique : *" qui est attesté, certifié conforme à l'original " ; " qui est véritablement de l'auteur auquel on l'attribue " ;*

- Identification : *" action d'identifier " ;*

1.Nouveau Petit Le Robert,dictionnaire de la langue française 1995

- Identifier : *" considérer comme identique, comme assimilable à autre chose ou comme ne faisant qu'un " ; " reconnaître du point de vue de l'Etat civil " ;*

- Identique : *" se dit d'objets ou d'êtres parfaitement semblables, tout en restant distincts "* [1].

Or, pour les techniciens, ces termes doivent être distingués. Et la distinction qui doit être faite n'est pas neutre.
De façon générale, il semble que la différence entre les deux notions se trouve dans le rapport avec la personne elle-même.

L'identification est permise par une représentation assez intime de la personne basée sur des éléments biotechnologiques.

L'authentification est basée sur des éléments souvent informatiques, sur un représentant sans rapport avec la personne elle-même.

3.1.2 Analyse terminologique des textes au regard de ces notions

3.1.2.1 Position commune en vue de l'adoption de la directive

La position commune en vue de l'adoption de la directive utilise les deux termes,en prenant,semble-t-il,en compte les différences existant entre ceux-ci.

Ainsi,si la signature électronique " simple " doit servir de méthode *" d'authentification "* [2], la signature électronique avancée doit *" permettre d'identifier le signataire "* [3].

Quant au certificat,celui-ci est défini comme une attestation électronique qui *" confirme l'identité de cette personne "* [4].

1.Nouveau Petit Le Robert,dictionnaire de la langue française 1995,p.160 et p. 11211.

2. *Position commune CE) N° 28/1999, précitée, article 2, 1)*

3. *Position commune CE) N° 28/1999, précitée, article 2, 2)*

4. *Position commune CE) N° 28/1999, précitée, article 2, 9)*

3.1.2.2 Projet de loi

Le projet de loi parle d'identification,à trois reprises :

- *" L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier sous réserve que soit dûment identifiée la personne dont il émane (...) " ;*

- *" La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose (...) " ;*
- *" 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. (...) ".*

3.1.2.3 Proposition de loi

La proposition de loi susvisée utilise le terme " authentification " : *" Un message électronique possède une valeur probatoire sous réserve du respect de deux conditions cumulatives : d'une part que soit possible l'authentification par une signature électronique fiable (...) ".*

3.1.3 Authentification ou identification

Le groupe de travail souhaite, en conséquence, attirer l'attention du législateur français sur la nécessité de prendre position sur l'utilisation du terme " authentification " et/ou du terme " identification " en prenant en considération les différences existant entre ces deux notions qui ne peuvent être utilisées indifféremment.

Les rédacteurs ont-ils réellement voulu parler d'identification ? Alors qu'aujourd'hui, la plupart des systèmes n'identifient pas mais authentifient.

Si le terme d'identification était conservé, et en admettant que ces termes recouvrent effectivement des réalités différentes prises en compte par les rédacteurs des projets, faut-il alors en tirer comme conclusion que les produits, s'ils répondent au critère de l'authentification, ne répondent pas à celui de l'identification ?

Dans ce cas, cela signifie-t-il que les moyens électroniques exis-

tant ne sont pas conformes à la directive ?

En effet,il semble que,intrinsèquement,la signature électronique ne puisse pas être un système d'identification.

Toutefois, il convient également de souligner que la signature manuscrite ne permet pas plus d'identifier que la signature électronique.

Enfin,il faut tenir compte,dans le cadre de cette réflexion,du fait que la personne qui utilise la procédure de signature électronique,l'utilisateur de la carte par exemple,ne sera pas forcément celle qui sera engagée.

Il semble que la position commune en vue de l'adoption de la directive ait pris en considération ce problème dans la mesure où le projet issu de cette position commune prévoit que le signataire peut-être *" toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou personne physique ou morale qu'elle représente "* [1].

Les enjeux du choix entre l'authentification et/ou l'identification ont une portée non négligeable qu'il convient impérativement de prendre en compte.

Le groupe de travail fait part de sa position sur cette problématique dans la dernière partie du livre blanc.

3.2 LA SIGNATURE ELECTRONIQUE, MOYEN DE NON-REPUDIATION

C'est avec le développement des réseaux internationaux ouverts, notamment que la fonction de non-répudiation a pris toute son importance.

Il est en effet essentiel de pouvoir opposer l'acte recouvert de la signature à la personne qui l'a émis.

La fonction de non-répudiation est essentielle pour le commerce.

---

1. Position commune CE) N° 28/1999, précitée, article 2, 3)

La non-possibilité de répudier la signature constitue en effet la force de l'engagement.

Si le lien entre le sujet de droit et l'objet de droit se fait du premier vers le second, l'objet doit toutefois pouvoir résister à la répudiation et la signature électronique doit garantir cette possibilité.

Les textes en matière de santé font clairement apparaître cette fonction nécessaire de la signature électronique.

En effet,ils prévoient que *" ainsi signés [avec une signature électronique], les documents électroniques (...) sont opposables à leur signataire "* [1].

3.3 LA SIGNATURE ELECTRONIQUE, MOYEN DE PREUVE DE L'INTEGRITE

Le rôle de la signature quant à l'intégrité du message ou plus généralement des données qui y sont associées est constamment réaffirmé.

Ainsi le Comité économique et social, dans son avis précité,estime que *" la signature électronique permet à celui qui reçoit des données transmises électroniquement de vérifier l'origine des données (authenticité) et de contrôler que les données originales sont complètes et inchangées (intégrité) "*.

Les projets de textes prennent en considération le nécessaire respect de l'intégrité du texte revêtu de la signature électronique.

Le projet de loi exige ainsi, pour que l'écrit électronique ait la même preuve probante que l'écrit papier, qu'il puisse être *" conservé dans des conditions de nature à en garantir l'intégrité "* [2].

1.Article 2 du décret n°98-271 du 9 avril 1998 relatif à la carte de professionnel de santé et modifiant le Code de la sécurité sociale et le Code de la santé publique, JO du 12 avril 1998, pages 5714 et 5715

2.Projet de loi du 1er septembre 1999 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique

Quant au texte de la directive issu de la position commune, il prévoit dans la définition même de la signature électronique, que celle-ci doit être *" liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable "* [1].

Les textes sur la santé prévoient, quant à eux, que *" la signature électronique produite par la carte de professionnel de santé"* garantit l'identité et la qualité du titulaire de la carte *" ainsi que l'intégrité du document signé "* [2].

3.4 LA SIGNATURE ELECTRONIQUE ET LE "REJEU"

En dehors de ces différentes fonctions essentielles de la signature,il faut évoquer la procédure dite de " rejeu ".

Cette procédure, mise en place dans le cadre du transfert dématérialisé des données fiscales et comptables à l'administration[3], permet d'assurer l'unicité des documents et, en cas de contestation,de pouvoir le vérifier.

1. Position commune CE) N° 28/1999, précitée, article 2, 2)1.Note du 14 mars 1996 de la DGI relative à la procédure de transfert des données fiscales et comptables (TDFC)

2. Article 2 du décret n°98-271 du 9 avril 1998 relatif à la carte de professionnel de santé et modifiant le Code de la sécurité sociale et le Code de la santé publique

3. Note du 14 mars 1996 de la DGI relative à la procèdure de transfert des données fiscales et comptables (TDFC)

Outre que la signature constitue un moyen de preuve (preuve du consentement, preuve du paiement, etc.), la possibilité d'apporter la preuve de la signature électronique et de conserver cette preuve est essentielle dans le développement de la signature électronique et des différents enjeux qui y sont liés.

C'est donc naturellement dans le cadre plus général de la preuve que s'insèrent les dispositions relatives à la signature électronique.

Le projet de loi indique clairement que la signature électronique participe à la preuve d'un message électronique puisqu'il dispose que *" 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 "* [1].

4.1 LES REGLES EN MATIERE DE PREUVE APPLIQUEES A LA SIGNATURE ELECTRONIQUE

4.1.1 La prééminence de l'écrit

Les articles 1315 et suivants du Code civil réglementent la preuve en matière civile.

La majorité de ces articles érige en principe la supériorité de la preuve écrite préconstituée et signée, laquelle représente un moyen de preuve parfait.

De plus, certains actes doivent être soumis à un formalisme particulier : certains doivent être établis par acte authentique[2] et d'autres seront nécessairement des actes sous seing privé[3] pour

1.Projet de loi du 1er septembre 1999, précité, article 1er, nouvel article 1316-1 du Code civil

2.Articles 1317 et suivants du Code civil

3.Articles 1322 et suivants du Code civil

ne citer que les deux catégories de types d'actes les plus répandus.

Toutefois,un certain nombre d'autres formalités ont été mises en place,tant par le Code civil que par d'autres textes.

On peut ainsi citer l'article 1326 du Code civil qui impose, pour les actes unilatéraux,l'engagement de payer une somme d'argent ou délivrer un bien fongible,que cet acte soit *" 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 "* [1].

Pour certains actes par ailleurs, un certain nombre d'originaux est exigé.

C'est notamment le cas de l'acte sous seing privé, qui n'est valable qu'autant qu'il a été fait d'originaux qu'il y a de parties à l'acte ayant un intérêt distinct.[2]

L'obligation imposée par certains textes d'établir des originaux pose inévitablement problème au regard de la signature électronique.

Peut-on toutefois réellement dire que le document électronique, revêtu d'une signature électronique, fait obstacle à l'existence d'un original ?

Ainsi,M.Caprioli écrit que *" le document informatique transmis ou reproduit ne possède jamais le caractère original, son unicité et sa signature faisant défaut. En matière électronique, le système d'information ne transmet aucun original (ce dernier reste en mémoire chez celui qui crée l'enregistrement), mais une simple copie dont la reproduction et la diffusion peuvent être infinies "*.[3]

Enfin, l'article 1341 du Code civil pose une exigence essentielle en matière de preuve civile dans la mesure où il exige qu'un écrit soit passé pour tous les contrats ayant un objet dépassant une somme ou valeur fixée par décret.

1.Article 1326 du Code civil

2.Article 1325 du Code civil

3.Eric A.Caprioli, Variations sur le thème du droit de l'archivage dans le commerce électronique, Petites Affiches, 18 et 19 août 1999

Cette somme a été fixée, en 1980, à 5 000 francs,et est toujours restée inchangée.[1]

Le maintien de ce seuil a d'ailleurs été,à de multiples reprises,critiqué,notamment par le Conseil National et du Titre qui écrivait, en 1997, qu'*" il convient au minimum d'élever le seuil réglementaire fixé à 5 000 F par le décret de 1980 au-dessus duquel un écrit est exigé pour les actes civils ".*[2]

Toutefois, si la preuve littérale, à savoir l'écrit signé par son auteur, présente une force probante très importante, un certain nombre d'évolutions législatives et jurisprudentielles ont modifié quelque peu les données.

4.1.2 L'assouplissement des règles de preuve

La règle de l'écrit préconstitué a été atténuée par quelques assouplissements du régime de la preuve, mis en place par les articles 1347 et 1348 du Code civil.

Trois exceptions principalement existent donc en la matière.

Tout d'abord, la règle de la préconstitution nécessaire de l'écrit reçoit exception lorsqu'il existe un commencement de preuve par écrit.[3]

Pour valoir commencement de preuve par écrit, il faut être en présence de trois éléments au
minimum :

- être en présence d'un écrit ;

- que cet écrit émane de celui contre lequel la demande est formée ou de celui qu'il représente ;

- que cet écrit rende vraisemblable le fait allégué.

1.Décret n°80-533 du 15 juillet 1980

2.Rapport du Conseil National du Crédit et du Titre sur les problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres, mars 1997, p.62

3. Article 1347 du Code civil.

Le commencement de preuve par écrit doit être complété par le demandeur au moyen d'autres éléments tels que des témoignages ou indices,et c'est ensuite au juge du fond d'apprécier, souverainement, si la preuve a été rapportée.

Un écrit électronique, revêtu le cas échéant d'une signature électronique, peut-il constituer un commencement de preuve par écrit ?

La jurisprudence n'a pas encore eu l'occasion de se prononcer sur ce point.

L'article 1348 par ailleurs met en place deux types d'exception au principe de la préconstitution de la preuve par écrit.

La première exception posée par l'article 1348 du Code civil concerne l'hypothèse où il y aurait eu impossibilité " matérielle ou morale de se procurer une preuve littérale de l'acte juridique " ou lorsqu'il y a eu perte du titre qui servait de preuve littérale à la suite d'un cas fortuit ou de force majeure.

Ce texte peut-il s'appliquer aux transactions dématérialisées dans la mesure où, de par leur nature même, il y a impossibilité d'établir un écrit ?

Seul le juge peut se prononcer sur l'application ou non de cette exception à l'écrit dématérialisé.

Précisons toutefois que l'impossibilité de se procurer un écrit *" est admise en ce qui concerne les ordres de Bourse reçus par téléphone. Les sociétés de Bourse peuvent rapporter par tous moyens la preuve de l'existence des ordres, notamment en enregistrant les conversations téléphoniques des clients qui passent des ordres de Bourse "*.[1]

La seconde exception mise en place par l'article 1348 du Code civil est celle aux termes de laquelle *" lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable "*, il n'y a pas alors nécessité de se préconstituer la preuve par écrit.

Le texte précise, par ailleurs, qu'*" est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support "*.

1.Ed. Francis Lefebvre,Alain Bensoussan, Informatique et Télécoms, 1997, n°603, p.206

Si la notion de caractère durable semble facilement appréciable, celle du caractère fidèle paraît beaucoup plus complexe à établir.

Il semble que la notion de " fidèle " puisse être rapprochée de celle de l'intégrité du document.

Sur le point de savoir si cette exception pourrait être appliquée aux transactions électroniques, certains y sont opposés.

Notamment, le Conseil National du Crédit et du Titre a fait remarquer que la notion de copie fidèle et durable vise en pratique *" la dématérialisation d'un document papier essentiellement aux fins d'archivage. La notion est donc inopérante ou inapplicable lorsqu'il n'existe pas d'écrit original : comment pourrait-on apprécier la fidélité à un original qui n'a jamais existé, si ce n'est sous forme électronique ? "* [1].

4.1.3 La liberté des conventions relatives à la preuve

4.1.3.1 La reconnaissance jurisprudentielle des conventions sur la preuve

En dépit de l'absence, jusqu'à ce jour, de dispositions relatives à la mise en place de conventions sur la preuve dans les textes, la jurisprudence a depuis plusieurs années reconnu la licéité de telles conventions.

En raison du caractère supplétif des règles relatives à la preuve, caractère reconnu unanimement par les tribunaux, les parties peuvent contractuellement mettre en place un système de preuve particulier.

Le contrat faisant la loi entre les parties[2], le contrat peut réglementer dans ce cadre les règles de preuve entre les parties.

Ces conventions de preuve devront toutefois respecter certains principes du droit civil,et notamment ne pas constituer une fraude à la loi en enfreignant des dispositions légales obligatoires et

---

1. Conseil National du Crédit et du Titre, " Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres ", mars 1997, p.60

2.Art.1134 du Code civil

en respectant,en outre,le principe du contradictoire[1].

Il faut citer dans ce domaine deux arrêts essentiels de la Cour de cassation rendu le 8 novembre 1989[2], lesquels ont consacrés définitivement la licéité des conventions sur la preuve.

Ces arrêts sont particulièrement intéressants dans la mesure où ils constituent également, dès 1987 avec l'arrêt de la Cour d'appel de Montpellier[3], la reconnaissance de la validité d'une signature électronique sous forme de code confidentiel concomitant à l'utilisation d'une carte.

Il s'agit des arrêts Crédicas.

4.1.3.2 Les arrêts Crédicas

C'est au terme d'un raisonnement probabiliste que la signature électronique a été reconnue par la Cour d'appel de Montpellier dans un arrêt en date du 9 avril 1987[4], ainsi que par la Cour de cassation dans deux arrêts du 8 novembre 1989[5].

Dans ces espèces, les tribunaux ont admis comme preuve d'une créance un paiement par carte de crédit, c'est-à-dire associant l'usage d'une carte magnétique et la composition concomitante d'un code confidentiel.

Il faut souligner que ces décisions ont été rendues dans des situations dans lesquelles la preuve était libre, les créances étant inférieures à 5 000 francs.

Toutefois, il n'en demeure pas moins que les tribunaux ont estimé que cette forme de signature électronique constituait un moyen suffisant pour la société de rapporter la preuve de sa créance.

En substance,les deux arrêts Crédicas rendus par la Cour de cassation ont statué de la façon suivante :

" Vu les articles 1134 et 1341 du Code civil ;

1.Ed. Francis Lefebvre,Alain Bensoussan,Informatique et Télécoms,1997, n°611 et 612,p.208
2.Cass.civ. I,8 novembre 1989,2 espèces,D 1990, Jurisprudence,p.369 et s
3.CA Montpellier, 9 avril 1987,précité
4.CA Montpellier, 9 avril 1987,précité
5.Cass civ 1ère,8 novembre 1989,2 espèces,Bull civ, n° 342,p.230

Attendu que la société Crédicas a consenti à Madame C... une ouverture de crédit utilisable par fractions, dans la limite de 5 000 francs (...) ; que le contrat a prévu l'usage par l'emprunteur d'une carte magnétique et la composition concomitante d'un code confidentiel valant ordre, pour l'organisme prêteur, de verser au vendeur le prix d'achat ; que, Madame C... ayant refusé de régler les sommes dont la société Crédicas s'estimait créancière (...) ;

Attendu que, pour rejeter la demande, le jugement attaqué retient que si pour les créances inférieures à 5 000 francs la preuve est libre, il est néanmoins nécessaire, quelles que soit les conventions des parties, que soient produits des éléments propres a entraîner la conviction du juge ; qu'il énonce que la simple production de documents dactylographiés émanant de la société demanderesse, ou, pour le moins et selon ses dires, d'une machine dont elle a la libre et entière disposition, est inopérante à constituer la preuve de l'engagement de rembourser consécutif à l'utilisation d'une fraction de l'ouverture de crédit consentie ;

Attendu qu'en statuant ainsi, alors que la société Crédicas invoquait l'existence, dans le contrat, d'une clause déterminant le procédé de preuve de l'ordre de paiement et que, pour les droits dont les parties ont la libre disposition, ces conventions relatives à la preuve sont licites, le Tribunal a violé les textes susvisés ".

Ces arrêts admettent donc non seulement la licéité des conventions sur la preuve, mais également la reconnaissance de la validité d'une signature électronique composée d'un code confidentiel et de l'utilisation concomitante d'une carte.

Comme l'avait écrit Martine Boizard, Docteur d'Etat en droit, à propos de l'arrêt de la Cour d'appel de Montpellier, *" les magistrats sont à l'évidence convaincus de la fiabilité du code secret dans la mesure où ils accréditent la " signature informatique " alors qu'il n'est allégué au demeurant aucun dérèglement du système informatique, ni perte de son numéro secret par le débiteur "* [1].

1.Commentaire de l'arrêt de la Cour d'appel de Montpellier du 9 avril 1987, JCP 1988, éd. G., II, 20984

4.1.3.3 La portée des conventions sur la preuve

C'est notamment dans le domaine bancaire que le développement des conventions relatives à la preuve a pris toute sa portée, et tout particulièrement dans le domaine des paiements par carte bancaire et des opérations de banque à domicile où *" les contrats contiennent des clauses suivant lesquelles les données enregistrées par les appareils automatiques ou par les banques constituent la preuve des opérations effectuées "* [1].

Ainsi, le Conseil National du Crédit et du Titre relevait, en 1997, que *" la dématérialisation des relations entre les banques et leurs clients s'inscrit le plus souvent dans un cadre contractuel : contrat de banque à domicile, contrat porteur carte bancaire, dispositions particulières et contrat cadre dans le domaine des échanges de données informatisées (EDI). C'est en application de ces conventions, et en particulier du contrat de banque à domicile et du contrat porteur carte bancaire, qu'un établissement de crédit est fondé, d'un point de vue juridique, à imputer le montant des opérations dont l'ordre a été donné par voie électronique (ordre de virement, opération de télépaiement, règlement par carte) au débit du compte de son client "* [2].

En matière de conventions sur la preuve et d'échange électronique plus particulièrement ,il a ainsi été écrit : *" Les entreprises concluent des " accords d'interchange " qui sont des contrats destinés à organiser l'utilisation de l'EDI (Echange de données informatisé) entre les parties. Ils ont pour objet d'indiquer quels sont les messages qui sont transférés par voie d'EDI et de prévoir comment résoudre les éventuels litiges concernant le contenu de chacun des messages dématérialisés qui ont été échangés.Il s'agit d'une technique contractuelle sinon sophistiquée du moins, très particulière, en ce sens qu'elle met en œuvre les règles légales relatives à la preuve qui ne sont pas habituellement incluses dans les contrats commerciaux "* [3].

Toutefois, si le recours aux conventions relatives à la preuve semble pouvoir être d'un grand secours dans le cadre de la signature de documents électroniques, son intérêt ne présente toutefois qu'une portée très relative dans la mesure où, dans le cadre

1. Conseil National du Crédit et du Titre, Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres, mars 1997. Pour d'autres exemples de conventions sur la preuve : voir ce rapport, p.69

2. Conseil National du Crédit et du Titre, " Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres ", mars 1997

3. Ed. Francis Lefebvre, Alain Bensoussan, Informatique et Télécoms, 1997, n°618, p.210

des réseaux ouverts, les occasions de conclure de telles conventions sont extrêmement limitées.

4.1.3.4 La reconnaissance légale des conventions sur la preuve

Le projet de loi, dans sa version du 1er septembre 1999, donne une assise légale aux conventions sur la preuve.

Le nouvel article 1316-2 du Code civil tel qu'il résulte du projet de loi dans sa rédaction du 1er septembre 1999 est en effet rédigé de la façon suivante :

" 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 ".

4.1.4 La charge de la preuve

Les règles relatives à la charge de la preuve pourraient également se trouver affectées par le changement de support des transactions.

Ainsi, il a été relevé que *" les règles générales peuvent s'avérer inéquitables dans un cas où le demandeur se trouverait face à un système de traitement de l'information " dominé " par l'autre partie, et n'aurait pas de moyen de preuve à sa disposition "*[1].

Précisons toutefois, en ce qui concerne la charge de la preuve, que les dispositions spécifiques à la consommation sont venues réduire les possibilités,dans le cadre des conventions sur la preuve,de porter atteinte aux principes de la charge de la preuve.

Ainsi, on trouve aujourd'hui, à l'article L.132-1 du Code de la consommation, en annexe, parmi une liste indicative et non exhaustive de clauses pouvant être regardées comme abusives si elles créent un déséquilibre significatif entre les droits et obligations de parties à un contrat,notamment la clause suivante :

1.Conseil National du Crédit et du Titre, " Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres ", mars 1997, p.48

" Clauses ayant pour objet ou pour effet :

(...) q) De supprimer ou d'entraver l'exercice d'actions en justice ou des voies de recours par le consommateur, notamment en obligeant le consommateur à saisir exclusivement une juridiction d'arbitrage non couverte par des dispositions légales, en limitant indûment les moyens de preuve à la disposition du consommateur ou en imposant à celui-ci une charge de preuve qui, en vertu du droit applicable, devrait revenir normalement à une autre partie au contrat " [1].

En d'autres termes, un contrat conclu entre un professionnel et un consommateur ne pourra avoir pour effet d'inverser la charge de la preuve,telle qu'elle est prévue à l'article 1315 du Code civil.

Enfin, le groupe de travail s'est interrogé sur l'opportunité de mettre en place une présomption,simple,dans le cadre de l'utilisation d'un mot de passe ou d'un code secret.

La mise en œuvre d'une telle présomption aboutirait à faire présumer l'engagement de la personne dés lors que le mécanisme de signature électronique aurait été activé.

Une telle présomption pourrait avoir des effets similaires aux conventions sur la preuve figurant dans les contrats porteurs de carte bancaire qui contiennent très souvent des clauses relatives à la force probante des enregistrements informatiques.

La mise en œuvre de présomptions de ce type aurait pour effet de renverser la charge de la preuve dans certaines circonstances, selon la personne sur laquelle pèse la charge de la preuve à titre originaire.

Cette proposition pourrait néanmoins se heurter à un obstacle : la notion de mot de passe n'est pas une notion juridique.

Soulignons toutefois que les termes de " code secret " ont en revanche été utilisés dans un texte récent. L'article 36 de la loi qui porte création d'une couverture maladie universelle [2] prévoit en effet qu'il sera possible de conditionner l'accès à une partie des informations visées par ce texte *" à l'utilisation d'un code secret "*.

1.Loi n°95-96 du 1er février 1995

2. Loi n°99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle, JO 28 juillet 1999, p.11229 et suivants

4.2 LA CONSERVATION DE LA SIGNATURE ELECTRONIQUE

4.2.1 Fonctions et durée

La conservation des documents correspond à deux finalités distinctes,qui peuvent s'appliquer de façon alternative ou cumulative :

- la conservation répond à une exigence légale ;
- la conservation répond à une exigence factuelle de conservation de la preuve.

Les délais de conservation seront fonction de la finalité à laquelle (ou auxquelles) ils obéiront :

- délais de conservation imposés par les textes dans le premier cas ;
- délais de prescription dans le second cas.

Les délais de prescription,sauf prescriptions plus courtes,sont de trente ans en matière civile[1] et de dix ans en matière commerciale[2]. En réalité,il existe un nombre important de délais plus courts. C'est le cas notamment en matière médicale[3] ou bancaire.A l'inverse, les délais de prescription sont en principe susceptibles de suspension ou d'interruption et sont donc susceptibles de perdurer au-delà de ces périodes.

4.2.2 Technique et impératifs juridiques

4.2.2.1 La situation au regard des textes actuels

En l'état actuel des textes, il semble donc que le support retenu

1.Article 2262 du Code civil

2.Article 189 bis du Code de commerce

3.En matière de données de santé transmises par voie électronique par exemple, l'arrêté du 9 avril 1998 notamment relatif aux conditions de réception et de conservation des feuilles de soins transmises par la voie électronique définit une durée de conservation de 3 ans pour chaque support d'enregistrement des messages transmis (arrêté du 9 avril 1998, JO du 16 avril 1998).

pour l'archivage des documents électroniques revêtus d'une signature électronique doit au minimum présenter les caractères suivants : être fidèle et durable, étant précisé que *" est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support "*[1].

Or il semble qu'aujourd'hui, seul un type de support satisfasse à l'ensemble de ces exigences : les disques optiques numériques non réinscriptibles de technologie WORM (Write Once Read Many).

Les disques WORM présentent la particularité suivante :leur état physique est modifié de façon irréversible pendant l'enregistrement.

L'utilisation de ces disques ne permet pas d'effacer une information une fois qu'elle y est enregistrée, ni,évidemment,d'en enregistrer une autre à la place.La présence de codes spécifiques sur ce type de disques rend la probabilité de modification quasiment nulle.

Dans ce cadre de l'archivage électronique, une norme[2] a été élaborée par l'AFNOR[3] en juin 1998 relative à la conception et l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des enregistrements stockés dans ces systèmes.

Cette norme a récemment fait l'objet d'une homologation[4], laquelle a pris effet le 20 juillet 1999.

Ce document,qui a simplement pour vocation de fixer des règles en matière d'archivage électronique, fournit un ensemble de recommandations concernant les mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques créés directement sous cette forme ou bien résultant d'un processus de numérisation d'un document papier.

Cette norme a vocation à s'appliquer exclusivement aux systèmes utilisant des supports de type non réinscriptible tels que le

1.Article 1348 du Code civil

2.Norme NF Z 42-013 "Recommandations relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes"

3.Association française de normalisation

4.Par décision n° 99-45 du 20 juin 1999 de l'AFNOR, JO du 23 juin 1999, p.10993

disque optique numérique de technologie WORM.

Mais cette norme met également en place des critères de fiabilité du système d'exploitation en imposant que le système dispose notamment de moyens de traçabilité et d'horodatage permettant de contrôler et de détecter les modifications ou altérations des enregistrements et de retracer l'historique des événements survenus dans le système.

4.2.2.2 Les nouveaux textes

Les projet et proposition français traitent tous deux de la conservation du document électronique.

Le projet de loi exige que l'écrit électronique soit *" établi et conservé dans des conditions de nature à en garantir l'intégrité "*, et non plus la fiabilité comme le prévoyait le précédent projet de loi.

La proposition de loi fait, quant à elle, dépendre la valeur probatoire du message électronique de la possibilité *" que soit assurée la conservation durable du message sous le contrôle du signataire "*.

Toutefois,il faut nécessairement,quel que soit l'état des textes en la matière, se poser la question de savoir si les technologies actuelles permettent d'assurer le délai de conservation légal.

Le papier dure bien au-delà de trente ans. En revanche, avec l'électronique,la conservation de dix ans ou de trente ans est-elle garantie ?

De plus,il faut souligner que le problème est non seulement celui de la conservation du support,mais également celui de la conservation de la signature.

Ainsi,en cryptographie,les choses évoluent très rapidement puisqu'aujourd'hui on arrive à casser des systèmes qui utilisent des clés de cryptographie de 512 bits. Qu'en sera-t-il dans dix ans d'une signature utilisant une clé de 1024 bits aujourd'hui dès lors que cette clé aura, entre temps, été cassée et qu'une autre personne pourra utiliser cette même signature et revendiquer l'engagement à son profit ?

Ceci entraîne donc les trois questions suivantes :

- qu'en est-il de l'évolution des technologies au regard de la preuve ?
- qu'en est-il de la conservation ?
- qu'en est-il de la personne qui conserve ?

Compte tenu de ces évolutions, le métier de " conservateur électronique " pourrait devenir dominant.

Il ne s'est toutefois pas dégagé de réponse forte à l'intérieur du groupe de travail sur la question de savoir si la conservation doit effectivement passer par la " notarisation " électronique, compte tenu notamment de la lourdeur du système à mettre en place.

Deux questions au minimum semblent devoir être résolues :

- comment règle-t-on la question de la fiabilité dans le temps ?
- comment règle-t-on la question de la relecture du support dans le temps ?

La proposition de loi exige, pour que la signature électronique ait une portée réelle dans le cadre de la signature d'un acte sous seing privé, que la signature consiste en l'usage d'un procédé " fiable " d'identification garantissant le lien avec l'acte auquel elle s'attache[1].

Mais cette notion de fiabilité n'est pas définie par le texte, et de façon générale par aucun texte.Or la fiabilité peut être entendue de façon absolue ou relative.

Dans quel sens le terme utilisé par le projet de loi doit-il dès lors être entendu ?

Le recours aux probabilités permet de suppléer, ne serait-ce que de façon partielle,à cette carence[2].

5.1 LA FIABILITE DE LA SIGNATURE ELECTRONIQUE AU TRAVERS DE DONNEES OBJECTIVES

Les moyens électroniques permettant d'accorder un niveau de fiabilité très élevé à la signature électronique sont nombreux aujourd'hui.

5.1.1 Les moyens de la fiabilité

Il convient à cette occasion de recenser de façon non exhaustive les différentes formes de signature électronique assurant un niveau de fiabilité particulièrement élevé :

- la carte à mémoire ou carte " à puce ".Cette carte présente une fiabilité certaine dans la mesure où elle ne peut être utilisée avant qu'une ou plusieurs clés correctes , un code confidentiel par exemple,n'aient été fournies ;cette carte doit être distinguée de la carte à mémoire simple ;

- la signature par empreinte digitale ;

1.Nouvel article 1322-2 du Code civil tel que rédigé dans le projet de loi du 1er septembre 1999
2.Le commerce électronique, Alain Bensoussan, Gazette du Palais, 18-20 octobre 1998, p.18 et s.

- la signature par ADN ;

- la signature par utilisation des autres moyens biométriques.

De façon plus générique,dans le cadre de l'étude de la fiabilité,il faut prendre en compte le " triplet " suivant : algorithme/clef/implémentation.

Cette fiabilité permise par les nouveaux moyens électroniques a d'ailleurs déjà été affirmée à plusieurs reprises,notamment par le Conseil National du Crédit et du Titre, qui écrivait en 1997 que outre l'utilisation d'un mot de passe ou d'un code confidentiel associé à l'utilisation d'une carte,procédé qui *" constitue un élément important de sécurisation des paiements sur réseaux ", " certains procédés permettent un niveau d'identification encore supérieur (reconnaissance dynamique de la signature, identification de la pupille, empreinte digitale), au point que l'on peut parler d'équivalents à la signature, électroniques "* [1].

Dans le même rapport, le Conseil National du Crédit et du Titre faisait, par ailleurs, remarquer que la généralisation de la carte à microprocesseur :

" constitue un progrès incontestable dans le domaine de la sécurité.

Elle a permis de réduire par quatre en 4 ans la fraude concernant les paiements par carte, le ratio " montant de la fraude/valeur des transactions " s'élevant à 0,03 % en France (soit un chiffre 5 fois inférieur à la moyenne mondiale) " [2].

Ne peut-on pas légitimement penser que lesdits procédés, et notamment les cartes à microprocesseur, permettent d'arriver à un niveau de fiabilité de la signature électronique plus élevé que pour la signature manuscrite ?

5.1.2 La fiabilité de la signature électronique en termes de probabilité

En termes de raisonnement probabiliste,le groupe de travail a été

1.Conseil National du Crédit et du Titre, Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres, mars 1997, p.71

2.Conseil National du Crédit et du Titre, Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres, mars 1997, p.15

l'occasion de faire un certain nombre de rappels et d'apporter un certain nombre de précision quant à la fiabilité de la signature électronique :

Ainsi :

- deux personnes ont la même empreinte originale avec une probabilité de 10^{-4} ;

- deux personnes ont la même empreinte génétique avec une probabilité de 10^{-9} .

Quant aux systèmes utilisant la cryptographie, il a été avancé[1] dans ce cadre les chiffres suivants :

* la probabilité pour que deux signatures prises au hasard soient identiques, avec des signatures RSA sur 1024 bits, est de 2^{-1024} soit environ 10^{-340}.

* la probabilité pour que les clés RSA de deux personnes ayant choisi leur clé par elles-mêmes soient identiques, étant donné que la densité de nombre premier est très forte (X/Log(X)),est de 2^{-1004} donc de l'ordre de 10^{-334}.

* Dans un processus de signature, la qualité de la fonction de " condensation " joue un rôle primordial,pour rendre " difficile "[2] la recherche de deux messages différents ayant même condensé, donc même signature.
+ avec SHA, qui est classiquement utilisé avec RSA 1024 bits, la taille est de 160 bits.La " difficulté " est alors de l'ordre de 2^{80} soit 10^{27} environ ;
+ avec un condensé de type MAC DES,donc 64 bits, la " difficulté " est de l'ordre de 2^{32} soit 10^{11} environ.

Ces chiffres démontrent sans aucun doute le degré de fiabilité très important des procédés électroniques de signature.

---

1. Jean-Claude Paillés à l'occasion du groupe de travail

2.Le terme " difficulté " est employé dans un sens de nombre d'opérations élémentaires à réaliser pour mener la recherche en utilisant le " paradoxe des anniversaires ", bien connu en cryptographie.Les chiffres donnés plus bas se réfèrent à une probabilité de succès de cette recherche de 1/2

5.2 LA SECURISATION DE LA SIGNATURE ELECTRONIQUE

5.2.1 Les moyens de sécurisation

5.2.1.1 La cryptologie

La cryptologie paraît être un moyen efficace de renforcer encore la fiabilité de la signature électronique ou peut-être plutôt de renforcer la confiance dans la fiabilité de la signature électronique.

Si la cryptologie était au départ réservée à la défense nationale et à la sécurité de l'Etat,son régime s'est depuis largement assoupli pour tenir compte des nécessités du commerce électronique et aujourd'hui,l'utilisation de la cryptologie est complètement libre pour certains types d'opérations.

C'est ainsi que l'article 28-1 de la loi du 29 décembre 1990[1] modifié en dernier lieu par la loi du 26 juillet 1996, établit un régime de liberté totale pour l'utilisation de la cryptologie pour les fonctions :

- d'authentification (moyen permettant de s'assurer de l'identité de l'expéditeur et de celle du destinataire d'un message) ;

- d'intégrité (moyen permettant de s'assurer que le message est arrivé complet, qu'il n'a pas subi de modification et/ou de prouver que le message est bien arrivé).

Est donc libre l'utilisation de moyens ou de prestations de cryptologie permettant d'élaborer ou de protéger une signature.

5.2.1.2 Les autres moyens

L'intervention d'un tiers neutre et indépendant peut être un moyen de renforcer la fiabilité de la signature électronique.

Ce tiers, désigné par les parties, peut en effet proposer les ser-

1.Loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications.

vices suivants :

" -identification fiable de l'émetteur et du destinataire (contrôle d'un code confidentiel, ...) ;
- intégrité des données transmises entre l'émetteur et le destinataire ;
- non-répudiation par l'émetteur et le destinataire des données transmises ;
- système de preuve opérationnel en droit français (conservation des preuves au moyen de la trace électronique laissée par un message ...) ;
- certification des échanges (horodatage complet ...) "[1].

Pour que le tiers puisse jouer correctement son rôle de " tiers témoin ",il doit toutefois présenter de véritables garanties de fiabilité vis à vis des parties.
Un autre moyen de sécurisation de la signature électronique peut également passer par la fourniture de moyens sécurisés ; ainsi, entre les professionnels de la banque, une norme internationale Etebac 5 a été mise au point[2].

5.2.1.3 La position commune en vue de l'adoption de la directive

Enfin, il faut signaler que la proposition de directive issue de la position commune prévoit un certain nombre de mesures visant à sécuriser la signature électronique, telles que la mise en place de certificats qualifiés et de systèmes d'accréditation volontaire[3].

Cette volonté se retrouve dans l'exposé des motifs du Conseil qui consacre un titre aux *" Mesures additionnelles destinées à améliorer le niveau du service de certification fourni par les prestataires de ce service ".*

Dans ce titre,le Conseil fait référence à l'extension de la respon-

---

1. Yann Bréban et Isabelle Pottier, Alain Bensoussan-Avocats, " Sécurité, authentification et dématérialisation de la preuve dans les transactions électroniques ", 1ère partie, Gazette du Palais 3-4 avril 1996, p. 4

2." Mémento guide Alain Bensoussan " Les télécoms et le droit ", Editions Hermès, 2ème éd., n° 16000 et s. relatifs à la preuve dans les télécoms "

3. Position commune CE) N° 28/1999, précitée, article 2, 10) et 13)

sabilité des prestataires de service au regard des certificats délivrés d'une part et d'autre part à *" la mise en place au niveau national de régimes volontaires d'accréditation destinés à améliorer le niveau de ces services "* et à l'obligation faite aux Etats membres *" d'instaurer un système adéquat de contrôle des prestataires de services délivrant des certificats agréés au public "*.".

5.2.2 Une ou plusieurs signatures ?

5.2.2.1 Signature manuscrite unique

En principe, chaque personne a une seule signature manuscrite. Mais dans certains cas, la loi ou la pratique exigent que cette signature manuscrite soit " sécurisée ".

Cette sécurisation peut revêtir différentes formes, de la plus simple à la plus formelle.Ainsi,la signature manuscrite devra parfois être accompagnée de la mention " bon pour ". Parfois, elle devra être reçue par des officiers publics, ce qui est le cas pour un acte authentique[1].

La signature manuscrite n'est pas différente selon qu'un acte présente une importance moindre ou au contraire décisive.

En revanche, il résulte clairement des textes comme des usages que plus un acte est important,plus sa signature est encadrée par un certain nombre de formalités devant être respectées, comme la présence d'un notaire.

La signature manuscrite est donc unique mais peut nécessiter la mise en place de certaines mesures qui s'y ajoutent, sécurisant ainsi la signature manuscrite.

5.2.2.2 Signature électronique unique ...

Ne pourrait-on fonctionner de la même façon en ce qui concerne la signature électronique et se prononcer ainsi pour l'existence d'une signature électronique unique ?

1.Article 1317 du Code civil

Une telle affirmation nécessiterait toutefois qu'un certain nombre de précisions et tempéraments soient apportés.

Ne retenir l'existence que d'une signature électronique suppose tout d'abord de bien séparer la signature elle-même du support.

Par ailleurs, ce n'est pas parce que la signature électronique est unique que toutes les signatures électroniques ont une portée identique.

En effet, à l'instar de la présence d'un officier ministériel dans le cadre d'une signature manuscrite, la mise en place de certificats numériques permet d'accorder une portée plus ou moins importante à la signature électronique.

Ainsi, si la signature électronique utilisée lors d'une demande de copie de fiche d'état civil et lors d'un virement bancaire est la même, il est clair qu'elle ne présentera certainement pas les mêmes caractéristiques.

En dehors des différents certificats de certification, la portée de la signature pourra également connaître des variations selon que la signature est faite à partir d'un dispositif uniquement logiciel ou à partir d'un dispositif également hardware[1].

Ne peut-on donc dire qu'il existe une seule signature électronique avec des moyens de sécurisation qui différent selon les circonstances,et notamment selon les intérêts en jeu.

Dans ce cadre, l'attention du groupe de travail est attirée sur le fait que si l'on peut éventuellement dire que la signature électronique est unique,il faut également préciser que la signature électronique est toujours identique et jamais pareille[2].

En effet :

- la signature électronique est toujours identique parce qu'elle vient toujours de la personne.Elle est donc unique ;

- la signature électronique n'est jamais pareille car elle dépend de deux variables :le support et une variable aléatoire pour éviter le rejeu.

---

1. Jean-Claude Dupuis

2.Alain Bensoussan

5.2.2.3 ... ou multiple ?

Dans l'hypothèse où il serait retenu l'existence de plusieurs signatures électroniques, un certain nombre de problèmes devrait alors être étudié.

Et, tout d'abord, il conviendrait de se poser la question de savoir s'il faut mettre en place une hiérarchie entre les différentes signatures électroniques.

C'est ce que semble préconiser le nouveau texte de directive issu de la position commune qui distingue :

- la signature électronique ;

- la signature électronique avancée[1].

Toutefois, on ne peut ignorer le fait que dans l'hypothèse où il y aurait plusieurs signatures électroniques, le marché risquerait alors d'être fragmenté, voire paralysé[2].

5.3 SUR LA PRISE EN COMPTE DE LA FIABILITE DE LA SIGNATURE ELECTRONIQUE

5.3.1 Par les professionnels

La signature électronique, une obligation de moyens ou de résultat ?

Il semble qu'aujourd'hui les professionnels aient tendance à ne s'engager que dans le cadre d'obligations de moyens.

Ainsi, dans le domaine des cartes bancaires, les sociétés émettrices desdites cartes ne s'obligent pas en termes d'obligation de résultat.

Avant de préconiser un changement de position,procédons à un rappel sur la distinction entre obligation de moyens et obligation

1. Position commune CE) N° 28/1999, précitée, article 2, 1) et 2)

2.David Ankri

de résultat.

Un tel rappel semble nécessaire dans la mesure où les techniciens envisagent souvent les obligations de moyens et de résultat de la façon suivante :

- l'obligation de moyens équivaut à un engagement sur les moyens, généralement traitée en régie ;

- l'obligation de résultat équivaut à un engagement sur les résultats,généralement traitée au forfait.

Cette analyse résulte d'une déviance.

Les notions d'obligations de moyens et d'obligations de résultat correspondent en fait à des processus de preuve.

Ces notions interviennent dans le cadre de l'administration de la preuve.

Lorsque l'obligation est une obligation de moyens,alors le créancier doit, en cas de difficulté, pour pouvoir engager la responsabilité du débiteur de l'obligation,démontrer :

- l'existence de l'obligation dont il est créancier ;

- l'écart entre cette obligation et la réalité ;

- la faute du débiteur dans l'exécution de ses obligations contractuelles.

En matière d'obligation de résultat en revanche,le créancier doit simplement démontrer l'obligation dont il est créancier et l'écart entre cette obligation et la réalité.

Il pourra alors engager la responsabilité du débiteur même si ce dernier n'a commis aucune faute. L'obligation de résultat peut-être, selon les cas,une responsabilité avec faute ou sans faute.

Etant donné le degré de fiabilité obtenu avec la signature électronique, on ne peut que s'étonner de ce que les engagements pris sur la base d'une telle signature ne soit que de moyens.

Et ce d'autant plus que les engagements pris sur la base d'une signature manuscrite sont le plus souvent des obligations de résultat.

Toutefois, il conviendrait de ne pas s'engager sans discernement sur la base d'un tel engagement.

Le périmètre de l'obligation de résultat devra être précisément défini et délimité.

Tout d'abord, il est clair que, en raison des conséquences juridiques attachées à la prise d'un engagement sur la base d'une obligation de résultat, les professionnels ne pourront s'engager que sur les opérations qu'ils maîtrisent et contrôlent.

Ainsi, lors d'une réunion du groupe de travail, a été soulevée la difficulté de garantir la chaîne dans le cadre des paiements par carte bancaire[1].

Cette remarque a été l'occasion de souligner que l'obligation de résultat ne doit pas être acceptée sur le processus dans son entier, mais sur les éléments du processus sous la responsabilité de la personne concernée par l'engagement en cause.

Par ailleurs,il a été rappelé que l'engagement de résultat ne pouvait être donné que par rapport à l'état de l'art à un moment donné.

C'est pourquoi le fait qu'il puisse exister un jour un moyen de frauder tel ou tel type de signature électronique,par exemple en " cassant " un code ne doit pas être un obstacle à la prise d'un engagement de résultat.

La limitation de l'obligation de résultat à l'état de l'art à un moment donné permet également de couper court aux difficultés liées à l'évolution des techniques.

Le seul impératif étant que le juge puisse se remettre dans les conditions dans lesquelles étaient les parties lors de la signature.

5.3.2 Par les textes

5.3.2.1 La position commune du 28 juin 1999 en vue de l'adoption de la directive

1.David Ankri notamment a fait remarquer que le terminal ou le système de paiement pouvaient être défaillants et la carte avoir fonctionné tout à fait normalement

Le nouveau texte semble prendre en compte la fiabilité de la signature électronique.

Ce texte prévoit, notamment, que la signature électronique ne devra pas se voir refuser l'efficacité juridique et la recevabilité comme preuve en justice au seul motif qu'elle se présente sous forme électronique ou qu'elle ne repose pas sur un certificat qualifié, quel qu'il soit, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature[1].

Toutefois,contrairement à la proposition de directive du mois de juin 1998,qui prévoyait que :

- " *Les Etats membres veillent à ce que les signatures électroniques reposant sur un certificat agréé délivré par un prestataire de services de certification (...) soient, d'une part, reconnues comme conformes aux exigences légales relatives à une signature manuscrite et, d'autre part, admises comme preuve en justice de la même façon que les signatures manuscrites* "[2],

le texte issu de la position commune ne prévoit pas clairement une telle équivalence

Or l'exposé des motifs du Conseil est lui très explicite puisqu'on trouve dans l'exposé des motifs les développements suivants : " *la signature électronique avancée est une signature offrant un haut niveau de sécurité qui se voit reconnaître à ce titre une validité équivalente à celle d'une signature manuscrite voir article 2, point 2, et article 5, paragraphe 1)* ".

Faut-il en conclure que l'on peut déduire de l'article 5 1. de la position commune qui dispose que :

" 1. Les Etats membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature :

a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier

et

---

1. Position commune CE) N° 28/1999, précitée, article 5, 2

2.Proposition de directive n° 98/C 325/04, précitée

b) soient recevables comme preuves en justice ",

que la signature électronique avancée qualifiée et sécurisée,pour la signature de documents électroniques,a la même validité juridique que la signature manuscrite pour des documents papier ?

5.3.2.2 Le projet de loi

A la différence du projet de loi du mois d'octobre 1998,le projet de loi actuel met en place un principe d'égalité entre l'écrit papier et l'écrit électronique.

De façon générale,le nouveau projet de loi accorde à l'écrit électronique la même valeur probatoire qu'à l'écrit papier en ces termes : " 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'intégralité ".

Concernant plus spécifiquement les actes sous seing privé, le projet de loi fait dépendre la force probante du document électronique de l'existence d'une signature électronique :*" Art.1322-1. - la même force probante est attachée à l'écrit sous forme électronique lorsqu'il constate des droits et obligations et qu'il est signé.".*

L'égalité entre les deux types de signature était loin d'être acquise.Cette position résulte en effet d'un changement d'orientation significatif du Conseil des ministres.

Le précédent projet de loi donnait en effet à la signature électronique une valeur inférieure à la signature manuscrite. Ce projet de loi,en date du 29 octobre 1998,disposait dans son article 2, qu'*" il ne peut être prouvé par écrit électronique contre et outre un écrit rédigé sur des registres ou papiers quelconques et signé par les parties ".*

Concernant la signature électronique spécifiquement,il faut toutefois signaler que le projet de loi, s'il précise que la signature nécessaire à la perfection d'un acte sous seing privé peut être électronique,précise toutefois 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 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." [1].

5.4 LA POSITION DU GROUPE DE TRAVAIL

5.4.1 La supériorité de la signature électronique sur la signature manuscrite

Il semble qu'aucune signature électronique ne soit sûre à 100%. Mais la signature manuscrite ne l'est pas non plus,loin de là.

Si l'opinion semble majoritairement penser que la signature manuscrite est plus sûre que la signature électronique,il n'y a pas de fondement logique à cette croyance.

Notamment, de façon très manifeste, une signature manuscrite est beaucoup plus facile à reproduire qu'une signature électronique.

D'ailleurs le législateur, conscient des faiblesses de la signature manuscrite, même dans le cas d'un acte authentique, a mis en place une procédure de vérification d'écriture qui impose au juge de procéder à la vérification d'écriture si l'une des parties dénie l'écriture qui lui est attribuée ou déclare ne pas reconnaître celle qui est attribuée à son auteur[2,3].

Il résulte des données techniques telles qu'exposées précédemment que la signature électronique est bien plus fiable que la signature manuscrite. Avec la signature électronique, les risques de fraude sont minimes, largement moindres qu'en présence d'une signature manuscrite.

Il paraît par ailleurs important de souligner qu'il n'est pas impé-

---

1.Projet de loi du 1er septembre 1999, précité, article 3

2.Article 285 et suivants du Nouveau code de procédure civile

3.Procédure d'inscription de faux pour les actes authentiques :article 1319 du Code civil et article 285 et suivants du Nouveau code de procédure civile

ratif, pour que la signature électronique puisse avoir une valeur juridique,qu'elle soit nécessairement certifiée.La signature électronique est suffisamment fiable pour se suffire à elle-même.

Mais il faut également préciser que le fait de mettre en place des procédures de certification de la signature électronique ne signifie pas que celle-ci présente des garanties moins importantes que la signature manuscrite. D'ailleurs, des procédures similaires de certification de la signature manuscrite existent.

En effet, lorsque deux personnes entendent conclure un acte sous seing privé à distance, et plus encore s'il s'agit d'un acte authentique, l'intervention d'un tiers certificateur, le notaire généralement,est alors requise.

La volonté de reconnaître à la signature électronique une valeur intrinsèque est d'ailleurs contenue dans le texte issu de la position commune qui impose aux Etats membres de veiller à ce que la signature électronique qui ne repose ni sur un certificat ni sur un dispositif particulier de création soit néanmoins revêtue d'une force probante certaine.

Comment dans ces conditions ne pas reconnaître à la signature électronique une fiabilité supérieure, ou au moins équivalente, à la signature manuscrite ?

Le groupe de travail souhaite que soit prise en compte cette équivalence entre signature manuscrite et signature électronique, avec toutes les conséquences de droit et de fait qui peuvent y être attachées.

5.4.2 Le rôle de l'Etat

Le groupe de travail s'est interrogé sur la question de savoir si les paramètres régissant la fiabilité de la conservation de la signature électronique devaient être définis par le marché ou par l'Etat ?

Un consensus au sein du groupe de travail a été trouvé à la suite d'une réflexion de Murielle Bergès pour laquelle la solution est à mi-chemin :

- les principes généraux devraient être fixés par l'Etat, qui donnerait les lignes directrices en matière de fiabilité ;

- les modalités pratiques seraient laissées au marché (y compris naturellement les aspects garantie et sécurité).

Par ailleurs, l'Etat ne devrait-il pas inciter les industriels à respecter la norme NF Z 42-013 sur la conservation ?

Dans le cadre de cette réflexion sur le rôle de l'Etat, le groupe a été amené à s'interroger sur l'éventualité d'un service universel de disponibilité en matière de signature : l'Etat doit-il mettre en place un tel service universel assorti de l'obligation de remise de carte gratuite ?

La position qui s'est dégagée du groupe de travail a été la suivante :

- les lignes minimales directrices en matière de signature doivent être définies par l'Etat ;
- le marché doit mettre au point les modalités pratiques ;
- l'Etat doit assurer un service universel en matière de signature électronique ;
- l'Etat doit assurer l'interopérabilité des certificats.

Enfin, le groupe de travail s'est interrogé sur le rôle de l'Etat quant à la préconisation de certaines solutions, qui lui paraîtraient plus fiables que d'autres.

Le groupe de travail pense que l'Etat devrait se prononcer, ne serait-ce qu'à titre d'information,sur ce point et préconiser, dans ce cadre, l'utilisation des cartes à microprocesseur, lesquelles semblent être,parmi les moyens de signature électronique accessibles à tous, une des technologies les plus fiables, voire la technologie la plus fiable.

5.4.3 Les préconisations du groupe de travail pour une protection optimale des utilisateurs

5.4.3.1 La dimension économique

Le groupe de travail estime important de mettre en place des solutions techniques permettant un large accès à la signature électronique.

Il ne faudrait en effet pas que la signature électronique connaisse un développement moindre en raison du coût généré par son "utilisation " alors qu'elle présente une fiabilité supérieure à celle de la signature manuscrite.

Le groupe de travail a voulu insister sur ces données économiques ;la signature a,de tout temps,été utilisée par tous,quelle que soit la situation économique de la personne.

La signature électronique doit rester dans cette même ligne : il serait en effet intolérable que,pour des raisons économiques,elle soit réservée à une partie de la population.

La prise en compte de cet impératif correspond d'ailleurs aux souhaits exprimés par Monsieur le Premier ministre Lionel Jospin dans son discours à Hourtin le 26 août 1999 aux termes duquel il déclarait : *" Un internet démocratique, c'est aussi un internet moins coûteux ".*

Déjà au mois de mars 1998,le Comité économique et social[1] s'exprimait de la façon suivante : *" à relativement brève échéance, tous les citoyens devraient pouvoir disposer d'un moyen (carte bancaire, carte de sécurité sociale, etc.) leur permettant de signer par voie électronique. (...) "*

La solution d'une carte délivrée par les services publics pourrait être la solution à défaut,pour les personnes ne pouvant acquérir une signature électronique auprès des industriels.

Selon le groupe de travail, il faudra prévoir une sorte de service universel de signature électronique.

5.4.3.2 Les nouveaux textes

On ne peut que se réjouir de l'intervention de l'Etat dans la mise en place de nouvelles règles prenant en compte les évolutions technologiques et mettant en place un cadre facilitant les échanges électroniques.

1.Avis du Comité économique et social du 25 mars 1998 sur la " Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions :Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et le chiffrement ", JOCE C 157 du 25 mai 1998, p.1

Toutefois, le groupe de travail souhaite que les textes finaux se prononcent clairement sur les notions d'authentification ou d'identification.

Sur ce point, la position majoritaire qui s'est dégagée du groupe de travail, lequel n'a pu aboutir à un consensus, est la suivante : en l'état de l'art,une signature électronique n'identifie pas directement une personne.

En revanche,la signature électronique renvoie à un porteur identifié et la mise en œuvre du mécanisme lié à la signature électronique permet l'identification.

De plus, le groupe de travail estime qu'envisager la présence de tiers de confiance sans identification n'est pas cohérent.

En fait, un numéro " ID ", ou numéro d'identification, pourrait apparaître comme une passerelle entre l'identité (nom/prénom) et l'identification.

La situation serait similaire à celle de la signature manuscrite, voire plus sûre dans la mesure où il pourrait y avoir un intermédiaire.

Par ailleurs, il faudra selon le groupe de travail tirer les conséquences de la fiabilité de la signature électronique.

C'est en partie ce à quoi s'attachent les nouveaux textes.C'est ce à quoi les professionnels devront également s'attacher, aidés par ces nouveaux textes,afin d'amener les utilisateurs à une confiance totale dans la signature électronique.

Le groupe de travail s'est enfin interrogé sur l'opportunité de mettre en place une présomption[1] lors de l'utilisation d'un mot de passe ou code secret, ou plus généralement, lors de l'utilisation d'un des mécanismes d'activation de la signature électronique.

Ce point mériterait,selon le groupe, d'être étudié.

1.Voir ci-dessus dans le titre " la charge de la preuve "

5.4.3.3 La mise en place de procédures spécifiques

Il est proposé par le groupe de travail de réfléchir à l'opportunité de mettre en place un certain nombre de procédures qui permettraient de renforcer la sécurité des transactions faites par le biais d'une signature électronique.

Tout d'abord, il pourrait être envisagé de créer un label, ou simplement une reconnaissance signalétique de valeur, pour les cartes à puce présentant un degré de fiabilité suffisant notamment.

Il serait opportun selon le groupe de travail que l'Etat encourage les industriels à s'organiser autour de label, plutôt que de laisser des labels " sauvages " se développer au détriment de l'utilisateur de la signature électronique.

Par ailleurs, la mise en place de procédures spécifiques de sanctions pourrait renforcer le caractère sécuritaire des transactions faites par signature électronique et le développement subséquent de celles-ci.

De telles procédures pourraient consister, par exemple, en l'instauration de lourdes sanctions en cas de fraude dans la délivrance des certificats numériques.

Afin d'augmenter l'acceptabilité des systèmes de signature électronique et d'assurer la sécurité, il pourrait également être envisagé de rendre obligatoire la souscription d'une assurance professionnelle pour le fournisseur du système de signature électronique.

Le groupe de travail estime toutefois majoritairement qu'il serait préférable de laisser aux industriels le choix entre souscrire ou non un tel contrat, tout en recommandant fortement à ces derniers de s'assurer au niveau professionnel dans le cadre de ces nouveaux services.

Il pourrait également être inclus,dans les contrats requérant l'utilisation d'une signature électronique, directement ou indirectement,des garanties contractuelles spécifiques.

Enfin,le groupe de travail a mis en exergue la nécessité d'organiser un système d'opposition, quel que soit le type de signature

électronique utilisé.

En revanche, à la question de savoir s'il doit être créé un fichier centralisé des cartes,et autres moyens de signature électronique, volées ou perdues,le groupe est resté très divisé.

PRECONISATIONS DU GROUPE DE TRAVAIL

n MISE EN PLACE D'UN SERVICE UNIVERSEL DE SIGNATURE ELECTRONIQUE

n INTEROPERABILITE DES CERTIFICATS DE SIGNATURE ELECTRONIQUE

n PRISE EN CONSIDERATION DANS LES TEXTES DE LA DISTINCTION ENTRE AUTHENTIFICATION ET IDENTIFICATION ET DU FAIT QUE LA SIGNATURE ELECTRONIQUE NE PERMET PAS UNE IDENTIFICATION DIRECTE

n CREATION DE LABELS DE SIGNATURE ELECTRONIQUE

n MISE EN PLACE D'UN SYSTEME D'OPPOSITION COMMUN A TOUS LES TYPES DE SIGNATURE ELECTRONIQUE

n EXPRIMER CLAIREMENT LES CONSEQUENCES JURIDIQUES LIEES A L'EQUIVALENCE ENTRE SIGNATURE ELECTRONIQUE ET SIGNATURE MANUSCRITE

n FAVORISER LA TECHNOLOGIE DE LA CARTE A MICROPROCESSEUR DANS LA MESURE OU ELLE EST LA SOLUTION DE SIGNATURE ELECTRONIQUE LA PLUS OPERATIONNELLE EN L'ETAT DE L'ART

n RECOMMANDER AUX FOURNISSEURS DE SYSTEMES DE SIGNATURE ELECTRONIQUE DE SOUSCRIRE UNE ASSURANCE RESPONSABILITE CIVILE PROFESSIONNELLE COUVRANT LES RISQUES LIES A CETTE ACTIVITE

n FAVORISER LE RESPECT DE LA NORME NF Z 42-013 SUR L'ARCHIVAGE ELECTRONIQUE

n ENVISAGER LA MISE EN PLACE D'UNE PRESOMPTION LORS DE L'UTILISATION D'UN MECANISME D'ACTIVATION DE SIGNATURE ELECTRONIQUE

Le présent Livre blanc comprend les annexes suivantes :

- Annexe 1 : Référentiel légal,
- Annexe 2 :Divers,
- Annexe 3 :Bibliographie,
- Annexe 4 : Participants.

ANNEXE 1

REFERENTIEL LEGAL

- Projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique en date du 1er septembre 1999.

- Loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle.

- Position commune CE) N° 28/1999 arrêtée par le Conseil le 28 juin 1999 en vue de l'adoption de la directive 1999/.../CE du Parlement européen et du Conseil du ... sur un cadre communautaire pour les signatures électroniques.

- Décret du 14 avril 1999 (n°99-285) modifiant le décret n°86-318 du 3 mars 1986 portant création du Service Central de la Sécurité des Systèmes d'Informations.

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

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

- Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens de prestations de cryptologie.

- Décret du 9 avril 1998 (décret n° 98-271) relatif à la carte de professionnel de santé et modifiant le Code de la sécurité sociale et

le Code de la santé publique.

- Arrêté du 9 avril 1998 relatif aux spécifications physiques et logiques de la carte de professionnel de santé.

- Arrêté du 9 avril 1998 relatif aux spécifications physiques et logiques de la carte d'assurance maladie et aux données qu'elle contient.

- Arrêté du 9 avril 1998 relatif aux feuilles de soins utilisant un support électronique.

- Arrêté du 9 avril 1998 relatif aux conditions de réception et de conservation des feuilles de soins transmises par la voie électronique, aux modalités d'envoi des messages adressés en retour et aux conditions d'exercice du droit d'accès et de rectification aux données contenues dans ces documents électroniques.

- Arrêté du 9 avril 1998 relatif aux conditions d'émission et de gestion des cartes d'assurance maladie.

- Arrêté du 13 mars 1998 définissant les dispositions particulières qui peuvent être prévues dans les autorisation de fourniture d'un moyen ou d'une prestation de cryptologie.

- Arrêté du 13 mars 1998 définissant le modèle de notification préalable par le fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis à autorisation.

- Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes.

- Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes.

- Arrêté du 13 mars 1998 fixant le tarif forfaitaire pour la mise en oeuvre des conventions secrètes au profit des autorités prévues à la loi du 29 décembre 1990.

- Décret du 24 février 1998 (décret n°98-101) définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie.
- Décret du 24 février 1998 (décret n°98-102) définissant les

conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi du 29 décembre 1990.

- Décret du 30 décembre 1997 (décret n°97-1321) relatif aux documents ouvrant droit aux prestations de l'assurance maladie et modifiant le Code de la sécurité sociale et le Code de la santé publique.

- Article 28 de la loi du 29 décembre 1990 (loi n°91-1170 sur la réglementation des télécommunications modifiée).

ANNEXE 2

DIVERS

- Société de l'information : discours du Premier ministre à l'Université d'été de la communication, Hourtin, 26 août 1999, http://www.internet.gouv.fr.

- Proposition de loi visant à reconnaître la valeur probatoire d'un message électronique et de sa signature,3 mars 1999.

- Avis du Comité des régions sur la " Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques ",14 janvier 1999.

- Avis du Comité économique et social sur la " Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques ", 2 et 3 décembre 1998.

- Projet de loi relatif à l'adaptation du droit de la preuve aux nouvelles technologies en date du
29 octobre 1998.

- Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, présentée par la Commission le 16 juin 1998,98/C 325/04.

- Avis du Comité économique et social sur la " Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions :Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et le chiffrement ", 25 mars 1998, JOCE C 157 du 25 mai 1998.

- Avis du comité des régions sur la " Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions intitulée " Une initiative européenne dans le domaine du commerce électronique ", 12 mars 1998.

- Cour de cassation, 1ère chambre civile , 8 novembre 1989, 2 espèces,D 1990,jurisprudence, p.369 et s.

- Cour d'appel de Montpellier, 9 avril 1987, 1ère ch., JCP, éd. G, 1988,II,20984.

ANNEXE 3

BIBLIOGRAPHIE

- " La signature électronique : un nouvel art de vivre ", Alain Bensoussan et Isabelle Pottier, Le médecin généraliste, supplément au n° 1970, 28 septembre 1999, p. 14 et s.

- " Variations sur le thème du droit de l'archivage dans le commerce électronique ", Eric A.Caprioli, Petites Affiches, 18 et 19 août 1999.

- " Le droit de la preuve : la signature électronique ", Alain Bensoussan, Technologie & santé, n° 36, avril 1999, p. 99 et s.

- " Cryptologie et signature électronique, aspects juridiques ", Alain Bensoussan et Yves Le Roux, Editions Hermès 1999.

- Le commerce électronique, Alain Bensoussan, Gazette du Palais, 18-20 octobre 1998, p. 18 et s. sur la preuve probabiliste notamment.

- " Internet, aspects juridiques ", Alain Bensoussan, 2è. éd., Editions Hermès, 1998.

- " Commerce électronique, Aspects juridiques ", Alain Bensoussan, Editions Hermès, 1998.

- " Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres ", Conseil National du Crédit et du Titre, mars 1997.

- " Informatique et Télécoms ", Alain Bensoussan, Editions Francis Lefebvre 1997.

- " Sécurité, authentification et dématérialisation de la preuve dans les transactions électroniques ", Yann Bréban et Isabelle Pottier, Gazette du Palais, 3 et 4 avril 1996, doctrine, p. 3 et s.

- Note du 14 mars 1996 de la DGI relative à la procédure de transfert des données fiscales et comptables (TDFC), JCP éd. E., n° 17, 25 avril 1996, n° 11581, p. 97.

- " La sécurité des réseaux, Méthodes et techniques ", J.-M.Lamère, Y. Le Roux, J.Tourly, Dunod informatique, Bordas, 1989.

- " Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ? ", J. Larrieu, Cahier Lamy du droit de l'informatique, novembre 1988 (H) et décembre 1988 (I).

ANNEXE 4

PARTICIPANTS

Liste des participants au groupe de travail sous la direction de :

Alain BENSOUSSAN et Charles Copin
Assistés par Marion DEPADT et Isabelle BEKHTI

Mme Anne CANTEAUT
Chargée de Recherche
INRIA

M. Pierre ANTONIO
Consultant
OZA

M. Bernard DAUNAS
Chef de Projet
OZA

M. Luc DEBORGIES
Responsable R&D Avancée
XIRING

Mme Laurence DUBOIS DE LIEGE
Juriste
Gie CARTE BLEUE

Mme Frédérique DURAND
Chef de Projet
Gie CARTE BLEUE

M. Gabriel PALOC-TAURY
Juriste
BULL

M. William TEULERY
Juriste
OBERTHUR CARD SYSTEMS

M. Jean LOPES
Responsable Centre des Réparations et Support Technique
INNOVATRON SERVICES

M. Philippe BEDERE
Maîtrise d'ouvrage SESAM-VITALE
CNAMTS

M. Marc BERTIN
Business Unit Director
OBERTHUR CARD SYSTEMS

Mme Séverine MAS-FOVEAU
Juriste International
GEMPLUS

M. Jean-Claude PERRIN
Product Line Manager
SCHLUMBERGER

M. Thierry COLLIN
Senior Manager Engineering
DASSAULT

M. Alain POTIER
Expert en "Cartes à Puce"
Institut de Recherche Criminelle Gendarmerie Nationale (IRCGN)

M. Laurent LETERRIER
Consultant
STERIA

M. Didier BARRE
Chef de Produit e-commerce
EXPERIAN

M. Michel-Paul BOURDIN
Directeur Domaine Sécruité
ATOS

Mme Murielle BERGES
Directeur-Adjoint du Groupement d'Intérêt Public " Carte Professionnel de Santé "
GIP-CPS

M. Jean-Paul THOMASSON
Directeur Marketing Smart Cards Product Division
STMICROELECTRONICS

M. Jean-Claude PAILLES
Chargé de Mission
FRANCE TELECOM

M. Bruno MICHAUD
Consultant Sécurité
MCO

M. Alain COUTY
Juridique et Moyens Généraux
EUROPAY FRANCE