REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE D'ORAN ES-SENIA

Faculté de droit

SIGNATURE ELECTRONIQUE «ETUDE DE DROIT COMPARE»

Mémoire de DPGS (diplôme de poste de graduation spécialisée) en droit international des affaires
Présentée et soutenue publiquement par:
HARIZ Asma

Sous la direction du professeur:

Mme ZENNAKI Dalila

Jury:

TRARI TANI Mostefa:	**Maître de conférences**	**Président**	**Université d'Oran**
ZENNAKI Dalila	**: Professeur**	**Rapporteur**	**Université d'Oran**
NACER Fatiha	**: Maître de conférences**	**Membre**	**Université d'Oran**

Année universitaire:2007-2008

SIGNATURE ELECTRONIQUE«ETUDE DE DROIT COMPARE»

REMECIEMENTS:

Je remercie pour l'aide et le soutien qu'ils m'ont apporté dans la rédaction de ce mémoire mes parents.

Je remercie enfin et plus particulièrement Mme le professeur Zennaki Dalila dont la collaboration m'a été fort précieuse.

SOMMAIRE:

PRINCIPALES ABREVIATIONS:

SE: Signature électronique

DE: Directive européenne

ISO: International Standard Organisation

COFRAC: Comité français d'accréditation

DCSSI: Direction centrale de la sécurité des systèmes d'information

CNCT: Conseil national du crédit et du titre

E.SIGN: Electronic Signatures In Global And National Commerce Act

UTA: Uniform Transaction Act

SiG.G:La loi fédérale allemande

PCS:Prestataire de services de certification

C.L.E:Contributions à la Littérature d'Entreprise

HSP:Hermes Science Publicat

INTRODUCTION:

L'Internet est un réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et des clients destinés à l'échange des messages électronique d'information multimédia et de fichiers (1).
L'Internet constitue un cadre d'expression de libertés fondamentales: liberté d'expression, la liberté de voyager, la liberté d'éditer et la liberté de commercer .Elles s'expriment principalement par la technique du web et de l'email ou courrier électronique. L'accès au réseau est ouvert à tout utilisateur ayant obtenu une adresse auprès d'un organisme accrédité.
Le développement de cette technologie qu'est l'internet bouleverse la conception classique des échanges et des relations entre les hommes.
Tout type d'information circule entre tous les utilisateurs sur l'ensemble de la planète de façon rapide et immatérielle .Les caractéristiques d'Internet qui en font un réseau mondial et complètement décentralise lui permettent de s'affranchir à la fois du temps et de l'espace. Le réseau ne connaît pas de frontière et aucune structure n'a vocation à le diriger globalement, il en découle une apparente liberté ainsi qu'une absence de contrôle administratif du comportement des différents acteurs en présence pour autant on ne peut parler de vide juridique sur internet.La loi existe elle pour être appliquer?
En 1976, deux chercheurs de l'Université de Stanford, Whitfield Diffie et Martin Hellman, publiaient un article qui allait révolutionner une branche des mathématiques dont la pratique était, jusqu'à ce jour, réservée à un cercle restreint d'initiés, la cryptographie.(2) Cette science, que Ronald Rivest définie comme celle de "la communication en présence d'adversaires" , a historiquement eu pour principale fonction de fournir aux Etats des moyens d'assurer la confidencialité des communications militaires ou diplomatiques.Ces moyens étaient, jusqu'en 1976, fondés sur un paradigme où l'émetteur et le récepteur d'une communication chiffrée se devaient de disposer d'une information commune , une clé secrète .

---

(1) Hafsi Samir, "Protection juridique du commerce électronique", mémoire de DEA en droit privé 2001-2002, p. 3,4.
(2)Jean-François Blanchette et FrançoisBanat-Berger, " La dématérialisation des actes authentiques de droit français", article publié sur le site:securinet.free.fr 2002, p. 4à5.

Cependant la nécessité pour les participants de s'entendre au préalable sur une telle clé commune réduit considérablement l'efficacité et la sécurité de tels systèmes de communications chiffrés.Dans leur article, Diffie et Hellman proposent un mécanisme mathématique inédit permettant à deux individus d'échanger des données chiffrées, avec la propriété étonnante qu'ils ne nécessitent pas de s'entendre au préalable sur une clé commune de chiffrement et de déchiffrement. Le mécanisme étant fondé sur la séparation de la clé unique en deux clés distinctes, une clé publique pour le chiffrement et une clé privée pour le déchiffrement, il est désigné sous le nom de cryptographie à clé publique, ou encore, cryptographie asymétrique.
Au –delà de ses applications au chiffrement des données, Diffie et Hellman suggèrent que leur mécanisme offre la possibilité de réaliser un "équivalent numérique" à la signature manuscrite, simplement en inversant l'ordre des clés: la clé privée devient la clé de la signature et la clé publique ,celle de vérification.Le mécanisme offre alors les assurances suivantes :d'une part, le message ainsi"signé" l'a bel et bien été par la clé privée correspondant à la clé publique utilisée pour la vérification; d'autre part,le message n'a pu être modifié après la "signature", sinon la vérification aurait échoué.
C'est l'explosion des technologies de l'Internet qui pose, au milieu des années 1990, le problème de la sécurisation du commerce électronique. La signature électronique, telle que proposée par Diffie et Hellman va alors soudainement se retrouver au cœur d'une série d'initiatives internationales visant à définir un cadre juridique pour les transactions électroniques suscitées par l'avènement supputée d'une société de l'information, où tant les relations commerciales que les relations entre l'Etat et le citoyen sont conduites par l'entremise de réseaux électroniques.
Contrairement à la signature manuscrite, la signature numérique, composée de chiffres, de lettres et d'autres signes, ne comporte aucun élément permettant de l'attribuer à une personne donné.Chaque utilisateur doit donc établir avec certitude l'identité de ses correspondants.C'est pourquoi on recourt a des services de certification, souvent, désignés comme" tiers de certification", qui disposent de la confiance de chacun et qui garantissent l'appartenance d'une signature à une personne. Comme le destinataire utilise la clé publique de l'expéditeur pour vérifier la signature électronique de ce dernier, la vérification suppose que le tiers certifie au destinataire que la clé publique qu'il utilise correspond bien à la clé privée de l'expéditeur signataire et que ce dernier est bien celui qu'il prétend être. Les tiers de certification délivrent donc des certificats d'authentification qui contiennent, d'une part, divers renseignements sur la personne dont on souhaite vérifier l'identité (nom, prénom, date de naissance) et, d'autre part, sa clé publique.Ces certificats sont généralement réunis dans des bases de données mises en ligne sur le réseau internet, ce qui permet à chacun d'y accéder facilement.

La signature numérique constitue donc un bloc de données crée à l'aide d'une clé privée, la clé publique correspondante et le certificat permettent de vérifier que la signature provient réellement de la clé privée associée, qu'elle est bien celle de l'expéditeur et que le message n'a pas été altéré.
La présente étude couvre plusieurs pays européens et non européens (Allemagne, Belgique, Danemark, Espagne, Italie, Luxembourg, Royaume Uni, CNUDCI, Etats Unis, France, Union Européenne, et L'Algérie). Pour chacun de ces pays, elle vérifie si la signature électronique bénéfice de la reconnaissance législative et en analyse les effets juridiques.Elle examine ensuite, le cas échéant, les conditions de validité de la signature électronique.
La directive européenne du 13 décembre 1999 va alors marquer une avancée significative dans la mesure ou elle va reconnaître en son article 5 l'admissibilité de la signature électronique.
Le but de cette directive était de promouvoir la sécurisation des transactions sur les réseaux numériques. Pour ce faire, elle attribue un minimum d'effets juridiques aux signatures électroniques dans le marché intérieur, et assure la libre circulation des produits et services attachées à celle-ci, notamment en prévoyant la liberté d'établissement des prestataires (1).
La loi française du 13 mars 2000 est venue modifier le droit français relatif à la preuve. Désormais, le doit reconnaît l'équivalence du support numérique dès lors qu'un certain nombre de conditions sont respectées.
Avec l'essor du numérique, la jurisprudence française a démontré, en la matière, une faculté d'adaptation appréciable.En effet, la cour de cassation a reconnu dès 1989 la validité de la convention de preuve introduite dans le contrat porteur des cartes bancaires, ce qui a permis au paiement électronique de se développer.De même, la photocopie, à qui la cour de cassation avait dénié toute portée juridique, a finalement été reconnue comme valant commencement de preuve par écrit. La recevabilité de l'écrit,et par extension de la signature, tend alors à se définir indépendamment de son support, et selon des critères précis que sont l'identification de son auteur et l'intégrité, qui seront les deux conditions essentielles posées par la loi du 13 mars 2000.

---

(1) Julien Esnault,"Signature électronique", mémoire de DESS du droit de multimédia et l'informatique, publié sur le site: www.signelec.com 2002-2003, p.4.

C'est pourquoi se posent les questions suivantes:
Quelle est la définition de la signature électronique ?
Quelle est la définition d'un certificat électronique?
L'homme peut-il s'exprimer dans les actes importants de sa vie autrement que sur du papier? en d'autres termes, à coté de l'écrit et de la signature traditionnels sur un document physique, y a-t-il place pour une autre forme d'écrit, électronique, numérique ?
Quelle est la responsabilité des prestataires de services de certification électronique?
Ces questions seront étudiées à partir de deux chapitres:

chapitre1) La création de la signature électronique laquelle se compose de deux

section:1) La reconnaissance juridique de le signature électronique, section2) Le

certificat électronique"pièce d'identité").

Chapitre2) Les effets juridique de la signature électronique lesquels se composent de deux section:1) La force probante de la signature électronique, section 2) La responsabilité des prestataires de services de certification électroniques.

CHAPITRE 1: LA CREATION DE LA SIGNATURE ELECTRONIQUE

La notion de la signature électronique n'avait jamais était définie par le droit. Cependant, avec la nécessite d'adapter le droit de la preuve à l'ère du numérique, les législations ont dû donner une définition de la signature.La signature manuscrite peut se définir comme une émanation de la personne (1).

Cette émanation est porteuse d'un double sens : d'une part, elle permet d'identifier la personne, puisque la signature est propre à chaque individu et, en théorie unique.

D'autre part, le fait d'apposer sa signature sur un acte juridique manifeste l'adhésion du signataire avec le contenu de l'acte.

L'identification doit, donc, absolument correspondre à celle de la personne, auteur intellectuel selon le droit. Afin de pouvoir s'assurer que la clé publique est réellement celle du détenteur prétendu,que celle-ci n'a pas été usurpée, il convient de le faire certifier par une tierce partie: le prestataire de services de certification électronique,qui va émettre un certificat.

Section1 : La reconnaissance juridique de la signature électronique

La plupart des pays développés sont entrain d'adapter leur cadre législatif à la signature électronique.

En Europe ,la directive européenne du 13 décembre1999 définit le cadre dans le quel doivent s'inscrire les lois nationales l'Italie et Allemagne ont modifié leur législation , la France le fait tout comme la plupart des autres pays européens,tels l'Espagne , le Luxembourg, le Royaume Uni, la Belgique, le Danemark (2).

---

(1) Julien Esnault, op.cit., p.7, 10.

(2) Guenièvre Bordinat, « Introduction a la notion de la signature électronique», article publié sur le site : www.signelc.com le 31 août 2002, p.1.

<u>Paragraphe 1</u> : La signature électronique dans la CNUDCI et l'Union Européenne et l'Algérie

1) la CNUDCI:

La première loi de la commission des Nations Unies pour le droit commercial international était la loi type sur le commerce éléctronique en 1996 qui offrait aux Etats membres des Nations Unies diverses méthodes pour supprimer les obstacles a l'utilisation des communications électroniques que contient leur droit commercial .

La loi type de la CNUDCI a était suivi par une loi spécifique sur la signature électronique. le texte de cette loi sur les signatures électroniques a été adopté le 05 juillet 2001 , et la définition qu'elle apporte de la signature électronique est la suivante : « le terme signature électronique désigne des données sous forme électronique, contenues dans un message de données ou jointes ou logiquement associées audit message ,pouvant être utilisées pour identifier le signataire dans le cadre des message de données et indiquer qu'il approuve l'information qui y est contenue » (article 2 ,a).

Cette définition attribue deux éléments fondamentaux à la signature électronique : l'identification du signataire et l'approbation de l'information contenue dans le message de données .L'approche retenue ici est donc une approche fonctionnelle.

2) L'Union Européenne:

Le 13 mai 1998, la Commission Européenne a présenté une proposition de directive dans un cadre communautaire pour les signatures électroniques. Le parlement européen l'approuvé le 13 janvier 1999, après avoir introduit quelques amendements. La Commission a donc présenté une proposition modifiée le 29 avril 1999, sur laquelle le conseil a adapté une position commune. Le 27 octobre 1999, Le Parlement européen a adapté quelques amendements formels à ce texte, sur lequel le conseil s'est prononcé le29 novembre 1999.

La directive européenne du 13 décembre 1999 définit la signature électronique par deux notions :

D'abord une définition générale de la signature électronique (article 2-1de la Directive) « La signature électronique correspond à une donnée sous forme électronique qui est jointe ou liée logiquement a d'autres données électroniques et qui sert de méthode d'authentification ».

Ensuite, elle propose une définition d'une catégorie particulière de signatures électroniques qu'elle qualifie de signatures électroniques avancées (article 2-2):

« En entend par signature électronique avancée, une signature qui satisfait aux exigences suivantes :

a- Etre liée uniquement au signataire.

b- Permettre d'identifier le signataire.

c- Etre crée par des moyens que le signataire puisse garder sous son contrôle exclusif.

d- Etre liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ».

Ces définitions données par la directive sont d'ordre technique et non fonctionnel (1).

Le point 1 des définitions vise certainement à englober ces différents mécanismes, sans toutefois leur reconnaître une valeur juridique comparable à celle de l'écrit papier signé manuscritement. On suppose que c'est a dessein que la définition fait état de « donnée servant de méthode d'authentification ».

L'authentification pouvant porter tant sur l'origine des données que sur leur intégrité, voir sur d'autres éléments.

---

(1) Julien Esnault, op.cit., p.5.

Par cette définition, la directive a voulu affirmer sa neutralité technologique en ne privilégiant aucun mécanisme particulier de signature électronique (1). La neutralité Technologique de cette définition n'est qu'apparente dans la mesure ou il ne fait pas de doute qu'actuellement, seules la technique de signature digitale fondé sur la cryptographie asymétrique répond a la définition de la signature électronique avancée.

3) L'ALgérie:

L'ordonnance n°75-58 du 26 septembre 1975 a été complétée et modifiée par la loi 05-10 du 20 Juin 2005.

Selon l'article 44 : cette ordonnance est complétée et modifiée par les articles 323 bis 1 et 327.

L'article 323 bis donne une définition nouvelle de la preuve par écrit:"la preuve par écrit résulte d'une suite de lettres ou caractères ou de chiffres ou de tout autre signe ou symbole doté d'une signification intelligible, quelques soient leurs modalités de transmission".

Les articles323 bis et 323 bis 1 contenus dans le code civil algérien sont presque la copie conforme des articles français (2).

---

(1)Santiago, Cavanillas Mugica, Vincent Gautrais, Didier Gobert, Rosa Julia, Barcelo, Etienne Montero, Yves Poullet, "Le commerce électronique"temps des certitudes, édition 2000, p.85.

(2) T.Gacem, " La signature électronique bientôt en vigueur en algérie-l'écrit et la signature électronique devront bientô avoir force probante en Algérie, article publié sur le site: www.algerie-dz.com2005, p.1.

Avec la croissance des échanges et de l'e-business, la sécurité devient de plus en plus cruciale. Le secteur de technologies de l'information et de la communication (ICT) a donc cherché une façon simple d'allier des aspects tels que l'identification des utilisateurs, la confidentialité et l'intégrité des messages, à un mode de communication infaillible. C'est ainsi qu'est née la signature électronique, le pendant électronique de la signature manuscrite (1).

La signature numérique est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité, par analogie avec la signature manuscrite d'un document papier (2). Un mécanisme de signature numérique doit présenter les propriétés suivantes:

Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature.

Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

Pour cela, les conditions suivantes doivent être réunies:

Authentique : l'identité du signataire doit pouvoir être retrouvée de manière certaine.

Infalsifiable:la signature ne peut pas être falsifiée. Quelqu'un d'autre ne peut se faire passer pour un autre.

Non réutilisable: la signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.

Inaltérable:un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.

Irrévocable: la personne qui a signé ne peut le nier.

---

(1) www.itmag-dz.com

(2) www.uneca.org

<u>Paragraphe2:</u> France et Etats-Unis

1) France:

La directive européenne du 13 décembre 1999 a été transposée dans la loi française 2001-230 du 13 mars2000 et dans le décret d'application 2001-272 du 30 mars2001.

La reconnaissance de la signature éléctronique en droit Français s'est effectué avec la loi du 13 mars 2000 portant « adaptation du droit de la preuve aux technologies de l'information et relative a la signature électronique ». Elle a été confirmée par le décret n°2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil relatif à la signature électronique.

La loi 2000-230 est venue modifier de manière substantielle le code civil. L'adoption de cette loi est en elle même un exploit, dans la mesure ou elle touche à des fondements du droit français, mais surtout parcequ'elle est le signe d'une réactivité du législateur à l'égard de l'émergence des nouvelles technologies et, notamment, de l'Internet .Entre le début de l'appropriation de l'Internet par le grand public et l'adoption de cette loi, trois années se seront écoulée.

L'adoption de la loi est l'occasion de définir la notion de « signature ». La signature est un élément indispensable à la perfection d'un acte juridique qui identifie celui qui l'appose et manifeste le consentement des parties.

Jusqu'alors le code civil ne comportait aucune définition de la notion de signature.

La signature électronique est défini comme consistant en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache (article 1316-4ccf) comme on pouvait s'interroger sur la notion de « fiabilité », les rédacteurs de la loi ont précisé que cette fiabilité était présumée jusqu' a preuve contraire (1).

---

(1) Anne Lise Vilarrubla,"Les apports de la signature électronique", article publié sur signelec.com, le21 octobre 2002, p.3.

L'article (1316-4 du code civil français) se veut indépendant de toute technologie et définit la signature par apport à ces fonctionnalités, contrairement a la directive.

La fiabilité d'un procédé de signature électronique sera présumée, jusqu'à preuve contraire sous les conditions données à l'article 2 du décret 2001-272.

Dès lors qu'une signature électronique sécurisée est mise en œuvre:

Elle doit être établie grâce à un dispositif sécurisé de création de signature électronique.

La vérification de cette signature doit reposer sur l'utilisation d'un certificat électronique qualifié.

L'article3.1 du décret 2001-272 du 30 mars 2001 fixe les exigences que doit satisfaire un dispositif sécurisé de création de signature électronique, ainsi :

« Un dispositif sécurisé de création de signature électronique doit :

1-Garantir par des moyens techniques et des procédures appropriées que les données de création de signatures électroniques :

a- Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée.

b- Ne peuvent être trouvé par déduction et que la signature électronique est protégée contre toute falsification.

c- Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.

2-N'entraîner aucune altération du contenu à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer ».

2) Etats-Unis:

Aux Etat- Unis le président Clinton a signé le 30 juin 2000 une loi fédérale intitulée « ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT ». Entrée en vigueur le 1er octobre 2000, elle harmonise au niveau fédéral les dispositions disparates adaptées par les états. Elle définit la signature électronique comme : «un son, symbole ou processus électronique joint ou associe logiquement à un enregistrement et exécuté ou adapté par une personne ayant l'intention de signer l'enregistrement ».

L’essence légale d’une signature est l’intention dans laquelle elle a été apposée plutôt que sa forme ou son support.

La définition de la directive européenne est approximativement identique, mais elle utilise le synonyme « authentifier »au lieu de « signer ».

<u>Paragraphe 3</u>: Luxembourg et Belgique

1) Luxembourg:

La loi du 14 août 2000 sur les signatures électroniques définit la signature électronique comme « un ensemble de données liées de façon indissociable à l’acte, qui en garantit l’intégrité ». (article6)

La loi adopte une approche neutre sur le plan technologique. Toutes les technologies peuvent être employées, dés lors qu’elles permettent la réalisation des fonctions caractéristique de la signature : l’identification du signataire et son adhésion au contenu de l’acte (1).

2) Belgique:

Le cadre juridique de l’utilisation de la signature électronique a été complété par la loi du09 juillet 2001 qui fixe certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.

Une première loi du 20 octobre 2000 avait pour objet de modifier le droit de la preuve en insérant dans l’article 1322 du code civil une nouvelle forme de signature.

Depuis lors « un ensemble de données électroniques pouvant être imputées à une personne déterminée et établissant le maintien de l’intégrité du contenu de l’acte ».

---

(1) www.uvcw.be

Encore faut- il que la fonction d'authentification de l'auteur de l'acte et de garantie de non altération du contenu de l'acte puissent être assurés. C'est là qu'intervient la deuxième loi , celle du 09/07/2001 : elle a pour objet de déterminer les cas dans lesquels une signature électronique aura véritablement cette force probante mais également de déterminer le cadre légal ou le fonctionnement des prestataires de services de certification.

Les lois luxembourgoises et belge visent toutes les formes de la signature électronique, mais elles divergent dans les effets qui leur sont reconnus.

<u>Paragraphe 4:</u>Allemagne et Italie

1) Allemagne:

Le législateur allemand évite de poser une définition de la signature électronique .En ce sens, il adapte la même position que les législations européens et française .Celle ci semble dictée par la volonté de rester ouvert aux évolutions technologiques.

Cependant cette apparence est trompeuse. Les textes envisagent un modèle précis de signature électronique, celui de la signature par cryptographie asymétrique.Ceci découle des termes employés tels que « clé de signature » « clé de vérification de signature » certificats, etc.

L'article 1er de la loi allemande du 16 Mai 2001 sur la signature digitale définit l'objet de la loi, qui est de poser les conditions générales auxquelles sont soumises les signatures digitales pour être considérées comme sûres et, pour que les faux en signature digitale ou la manipulation de données puisent être établis de manière fiable.

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

Elle ne traite que de la signature digitale qui est fondée sur la cryptographie asymétrique et qu'elle définit à l'article 2 comme « un sceau attaché à une donné numérique qui est produit par une clé privée, qui authentifie le propriétaire de la clé et établie l'intégrité des données au moyen d'une clé publique correspondante, fournie avec un certificat de clé, lequel est délivré par un prestataire de service de certification ou par l'autorité de contrôle » (1).

La loi allemande a donc fait un choix technologique, ce qui en soi n'est pas totalement critiquable car il faut bien reconnaître que ce mécanisme offre un niveau de sécurité élevé tout en ayant un coût limité. Il est par contre plus étonnant que la loi ne traite pas de la valeur juridique, notamment en droit de la preuve, à accorder à un document signé digitalement dans les conditions de cette loi. On peut probablement en conclure que les règles classiques du droit de la preuve du code Civil allemand continuent à s'appliquer.

2) Italie:

La loi italienne du 15 Mars 1997 (dite loi Bassanini) dispose d'une composante définissant les principes juridiques de fonctionnement de la signature et, d'un décret précisant le fonctionnement, les technologies et les assurances sécuritaires requises.

Cette loi a été précisée par un décret présidentiel N° 513 du 10 Novembre 1997, lequel définit la signature digitale comme : « le résultat de la procédure informatique fondée sur un système de clés asymétriques, une publique et une privée, de garantir l'origine et l'intégrité d'un document informatique ou d'un ensemble de documents et au destinataire, par l'intermédiaire de sa clé publique de vérifier ces deux éléments».

---

(1) www.senat.fr

D’après cette définition, le décret présidentiel est technique.

Allemagne et l’Italie sont actuellement les seuls pays ou un texte définit le régime juridique de la signature électronique.

Mais les textes allemand et italien ne reconnaissent que certaines formes de signature et leur accordent des effets différents.

Paragraphe5:Royaume-Uni, Espagne, Danemark

1) Royaume-Uni:

Le Royaume –Uni, avec «L' ELECTONIC COMUNICATION ACT 2000 »définit la signature électronique 'lorsqu'elle est utilisée a des fins judiciaires, comme un bloc de données électroniques :

a)Qui est incorporé ou logiquement associé à un message électronique.

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

2) Espagne:

Visant à simplifier et à encourager le recours aux signatures électroniques, la nouvelle loi espagnole sur les signatures électroniques (loi 59/2003) et elle entrée en vigueur le 20 mars 2004. La nouvelle loi définit la signature éléctronique et la signature électronique avancée en reprenant la même formulation que la directive européenne (1).

Cette loi permet également de modifier et d’ajouter certaines règles à la loi espagnole sur le commerce électronique (loi 34/ 2002) et à la loi sur la procédure civile espagnole (loi 1/2000).

---

(1) voir l'article 2 de la DE.

3) Danemark:

La loi sur les signatures électroniques du 31 Mai 2000 reprend la définition de la directive européenne, mais n'établit pas de distinction entre signatures électroniques, et « signature électronique avancée ».

L'objet de cette loi est de promouvoir l'utilisation sûre et efficace des moyens électroniques et de communication en fixant les exigences auxquelles elles doivent satisfaire.

Section2: Le certificat électronique (pièce d'identité)

Le certificat est au cœur du processus de signature électronique.

Il est porteur d'une valeur juridique puis qu'il va permettre l'identification de la personne, mais il a également une définition technique (1).

Un certificat de signature électronique est l'équivalent moderne des sceaux qui, dans l'antiquité, permettait de cacheter une lettre ou de signer un traité.

Il s'agit d'un document électronique composée de deux éléments distincts : une clef privée de signature grâce à laquelle le détenteur du certificat, et lui seul, peut créer des signatures électroniques, et une partie publique, qui rassemble à peu près les mêmes éléments qu'une carte d'identité professionnelle (nom et prénom de la personne, nom de l'entreprise..).

Les certificats de signature sont personnels et, sont souvent distribués sur des supports sécurisés : carte à puce (2) ou leur variante : clefs USB qui est un composant qui rassemble a la fois une carte à puce et son lecteur.

---

(1) Julien Esnault, op.cit. , p.11.

(2) Une carte à puce constitue un domaine de sécurité confiné ayant des capacités de traitements intéressantes.

Une clé est une valeur numérique unique qui fait partie de l'algorithme de chiffrement .Il s'agit d'une suite de caractères utilisés pour coder et décoder un dossier, la clé est utilisé pour chiffrer et déchiffrer un message. Mais les signatures électroniques utilisent la cryptographie « clé publique ».

La cryptographie est l'art de transformer des informations que seul les personnes autorisées peuvent lire .L'information est codée d'une façon à ce que seul le destinataire puisse lire ou altérer.

La cryptographie a clé publique se caractérise par l'utilisation de deux clés :

La clé privée permet de générer la signature, elle est secrète.

La clé publique est utilisée pour vérifier la signature électronique elle doit impérativement rester intègre.

<u>Paragraphe1</u>: **Le certificat électronique dans la CNUDCI et l'Union Européenne et l'Algérie:**

1) CNUDCI:

La loi type de la CNUDCI sur les signatures électroniques (2001) dans son article 2 alinéa – b) définit le terme certificat comme suit « le terme certificat désigne un message de données ou un autre enregistrement confirmant le lien entre signature et des données afférentes à la création de signature ».

2) L'Union Européenne:

D'après l' Union Européenne ,seules les signatures électroniques créees dans des conditions de sécurité optimale peuvent avoir la même valeur que les signatures manuscrites .En effet , cette équivalence est réservée aux « signatures électroniques avancées » basées sur un certificat qualifiée et crée par un dispositif sécurisé de création de signature .

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

Les titulaires des certificats sont des personnes physiques qui peuvent, le cas échéant, agir pour le compte d'une personne morale.

La directive ne mentionne aucune indication de durée de validité maximale pour les certificats.

L'annexe I de la directive européenne énumère les exigences relative aux certificats qualifiés. Ces derniers comportent nécessairement :"

a- Une mention indiquant que le certificat est délivré a titre de certificat qualifié.

b- L'identification du prestataire du service de certification, ainsi que les pays dans lequel il est établit.

c- Le nom du signataire ou un pseudonyme qui est identifié comme tel.

d-La possibilité d'inclure, le cas échéant, une qualité spécifique du signataire en fonction de l'usage auquel le certificat est destiné.

e- Les données afférentes à la vérification de la signature qui correspondent aux données pour la création des signatures sous le contrôle du signataire.

f- L'indication du début et de la fin de la période de validité du certificat.

g- Le code d'identité du certificat.

h-La signature électronique avancée du prestataire de service de certification qui délivre le certificat.

I- Les limites à l'utilisation du certificat, le cas échéant, et

J- Les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant."

Le législateur prévoit d'une part un certificat « qualifié » et d'autre part une signature « avancée », il a laissé la question ouverte en n'etablissant pas de lien (1).

3) L'Algérie:

Le nouvel article 323 du code civil Algérien est exactement identique à l'article français concernant la signature et l'écrit électronique .L'Algérie doit mettre en place une politique de certification complète de manière à ce qu'elle soit validée au niveau mondial par la création de tiers certificateurs (2).

Les signatures numériques sont sur le point de devenir un des principaux outils de la sécurité dans Internet. Le certificat identifie son propriétaire devant quelqu'un qui a besoin d'une preuve de l'identité du titulaire. Ainsi, les certificats numériques sont utiles dans une grande variété de situations. Ils peuvent servir pour la signature de documents de courrier électronique de manière à identifier et authentifier l'expéditeur de façon absolue (3).

Le certificat est émis, associé à l'outil. Il permet d'affirmer deux choses:

a) Le lien entre la personne et l'outil.

b) Que ce lien est toujours valide (c'est la durée de vie du certificat).

---

(1) Béatrice Jaluzot, Le recueil Dalloz N° 40 du 2004"transposition de la directive, signature électronique, comparaison franco-allemande", p. 2873.

(2) J.C.Monnier, "Il faut que l'Etat soit le moteur de développement", article publié sur le site www.itmag-dz.com dimanche 8 mai 2005, p.1.

(3) Fayçal Ben Amour, Les clés du commerce électronique, édition C.L.E Tunis, 2001, p. 156,157.

Les méthodes d'attribution de certificats électroniques en Algérie ne sont pas encore établies malgré l'existence de lois autorisant la dématérialisation des échanges électroniques comme le relèvent des spécialistes ,à l'image de Mme Fouzia Guessoum ,directrice générale de SG-Software qui a déclaré, lors d'une conférence conjointe au centre de presse du quotidien El Moudjahid ,avec le représentant de la société française AZZARIUS,Jean-Claude Monnier, qu'ils sont dans l'attente de la promulgation de ces textes,afin de pouvoir désigner l'agence de régulation ,le certificateur et comprendre comment procéder à l'attribution des certificats (1).

SG-Software, est une entreprise de services informatiques proposant des solutions dans le domaine de la gestion électronique des documents. En fait, fera-t-elle remarquer "la grande question qui se pose en ce moment en Algérie est comment parvenir à l'application de la dématérialisation des documents ". Le certificat électronique permet d'authentifier l'établissement concerné (Société, Banque, Ministère, etc.), afin de lui attribuer une signature électronique "propre" à lui, notamment lors des contrats et des protocoles d'accord, dans un souci de protection contre les tentatives de modification et de fraude, est-il expliqué. L'échange d'un document électronique entre deux entreprises sera"protégé", grâce à la signature électronique qui, selon eux, assure son authenticité et annule toute tentative de modification.

Les entreprises ont la possibilité de délivrer des certificats numériques à leurs employés et d'utiliser les certificats pour autoriser l'accès aux ressources du réseau, remplaçant ainsi les mots de passe et les noms d'utilisateurs. Les employés qui accèdent au réseau de l'entreprise à partir de leur domicile ou en voyage utilisent alors les certificats numériques pour s'identifier devant le pare-feu de l'entreprise (2).

---

(1) actualité.el-annabi.com

(3) Fayçal Ben Amour, op.cit., p. 158.

L'autorité de certification fournira les certificats numériques. Le degré de confiance à accorder à un certificat dépend de la rigueur du processus utilisé pour vérifier l'identité lorsque le certificat est émis.

Les certificats numériques ne sont pas encore normalisés ni universellement reconnus.

De nombreux organismes de délivrance différents existent et un certificat émis pour un navigateur donné peut ne pas être accepté par l'autre , chaque application ayant sa propre façon de traiter les certificats et tous les certificats n'étant pas interchangeables entre les applications.

Paragraphe2 : France et Etats-Unis

1) France:

Le décret du 30 Mars 2001 reconnaît deux types de certificats : le certificat électronique simple et le certificat qualifié. Le premier est un document qui se présente sous la forme électronique et qui atteste du lien entre les données de vérification de signature électronique et un signataire.

Le certificat électronique qualifié doit répondre à une série de critères définit par le décret(1).

Selon le décret 2001 – 272 du 30 Mars 2001 , le certificat électronique qualifié doit avoir été délivré par un prestataire capable de délivrer ce type de certificats et comporter certaines indications (article 6) , telles que :

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

b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans le quelle il est établit.

---

(1) Julien Esnault, op.cit., p.11.

c) Le nom du signataire ou un pseudonyme, celui ci devant alors être l'identifié comme tel.

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

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

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

g) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique.

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

Selon l'article 3 du décret français du 30 mars 2001, seul le prestataire de service de certification qualifié peut délivrer une signature électronique sécurisée, car il est le seul à mettre en œuvre un dispositif de création sécurisé.

Ce dispositif doit, en effet , avoir été certifié conforme soit par un organisme désigné par un Etat membre de la communauté européenne , soit par un service du premier ministre, la direction centrale de la sécurité des systèmes d'information dans les condition prévues par le décret du 18 avril 2002 (1). La certification sera l'aboutissement d'une longue série de vérifications et de tests .En effet le procédé de création de signature électronique devra d'abord faire l'objet d'une évaluation , puis d'une certification par un centre d'évaluation, devant lui même être préalablement agrée.

---

(1) Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, J.O.Numéro77 du31mars2001, p.5070.

Un arrêté français est paru le 31 mai 2002 désignant le centre français d'accréditation COFRAC pour accréditer les sociétés qui évalueront, pour deux ans les prestataires de certification électronique, mais il y a un autre arrêté du 26 juillet 2004 (en remplaçant l'arrêté du 31 mai abrogé), cet arrêté complète le décret 2002 et précise l'organisme chargé d'accréditer les organismes d'évaluation des prestataires de service de certification.

Concernant le cycle de vie d'un certificat, celui ci commence par le tirage des deux Clés, la clé publique et la clé privée .Il se poursuit par la demande du détenteur des clés de ce certificat, puis par la validation des justificatifs apportés. La phase suivante compte chronologiquement l'utilisation proprement dite des clés et du certificat, la validation dudit certificat et sa suspension ou sa révocation.

Le cycle s'achève avec l'expiration des clefs du certificat et recommence ensuite à la phase première (1).

Le certificat doit contenir plusieurs éléments : la version , le numéro de série ,le nom du porteur ,sa clef publique , l'algorithme utilisé ,les dates de validité, le nom de l'émetteur , l'identification de la politique de certification et la signature de l'émetteur .

Chaque personne qui souhaite obtenir un certificat doit, choisir le type de certificat souhaité (sur carte à puce ou clef USB) en fonction de l'offre de logiciel.Elle doit prendre contact avec l'autorité de certification pour connaître le contenu du dossier à constituer (plusieurs pièces justificatives).

Elle doit adresser le dossier constitué à l'autorité de certification.

---

(1) www.clic-droit.fr

Elle doit retirer un pli personnel à son bureau de poste (qui contient un code secret) et suivre la procédure indiquée dans ce courrier, suivre les instructions fournies par l'autorité de certification, qui peuvent inclure un déplacement physique dans ces locaux ou jusqu' a un bureau de poste pour justifier de l'identité du porteur.

Recevoir le support (la carte à puce ou la clef USB au choix), et l'installer sur un poste de travail connecté a l'Internet.

Enfin générer son couple clef privée, clef publique, et télécharger le certificat. Pour cela en général il faut se connecter sur le site web fourni par l'autorité de certification retenu par le bénéficiaire du certificat.

La page web permet alors de lancer la génération du couple de clefs (cette opération se déroule a l'intérieur de la carte à puce ou de la clef USB) et d'envoyer à l'autorité de certification la clef publique ainsi créée.

Il faut ensuite attendre de recevoir un e– mail de confirmation (notifiant que le certificat a été fabriqué par l'autorité de certification). Enfin il faut se reconnecter au site web de l'autorité de certification et télécharger le certificat (1).

Le délai total à prévoir pour cette opération (de la prise de connaissance du dossier au téléchargement du certificat) est d'environ 02 semaines.

En ce qui concerne l'autorité de certification : il s'agit d'un élément clef de la confiance, cette autorité est définie par ISO (2) comme suit : " l'autorité de certification est une autorité qui à la confiance d'un ou plusieurs utilisateurs pour générer et assigner des certificats. En option, l'autorité de certification peut générer les clefs des utilisateurs".

---

(1) www.achatpublic.com

(2) ISO, INTERNATIONAL STANDARD ORGANISATION:organisme qui s'occupe de l'établissement de normes internationales.

2 Etats-Unis:

Plusieurs différences essentielles existent aujourd'hui entre la législation française et américaine.

En vertue de la nouvelle législation française une signature électronique doit satisfaire la procédure d'identification pour être valable. Pour se faire la législation française parait suggérer que la certification doit être systématiquement utilisée.

Les différences entre la France et les États-Unis sur la question de la certification sont donc sensibles (1). D'une part, la législation Française exige la certification pour valider une signature électronique. A cet égard, la France a déjà commencé à définir le cadre dans lequel la signature électronique va opérer.

D'autre part, la législation aux Etats-Unis reste muette sur le sujet de la certification. Certains estiment que ce silence autorise tacitement l'utilisation de la certification.Une autre différence tient aux tiers certificateurs qui, en France, seront soumis au contrôle du gouvernement.

Aux Etats-Unis, ces prestataires de services sont souvent des sociétés privées telles que digital signature trust ou verusign.

La loi E-sign adopte les méthodes traditionnelles de vérification d'identité par un tiers comme la certification conforme par un officier assermenté (notarization) et la confirmation (acnowledgment). Elle permet que cette vérification soit effectuée par voix électronique.

---

(3) Laurence Birnbaum-Sacryet Florence Darques, "Signature électronique, comparaison entre les législations française et américaine", article publié sur signlec.com en avril 2001, p.3.

Cependant, en vertu d'E-sign la présence de l'officier public (notary) n'est plus requise pour que la vérification soit valable. E- sign précise que si une disposition légale exige qu'une signature soit certifiée ou confirmée, cette condition est remplie dès lors que la signature électronique de l'officier assermenté est jointe ou liée logiquement à la signature ou au fichier. Le principe classique de la certification conforme est préservé mais peut désormais être accompli par voix électronique.

La loi française 2000-230 du 13 mars 2000 traite également de l'acte sous signe privé et de l'acte authentique.

Les actes sous seing privé sont des accords signés par les parties au contrat, ils n'ont pas à être confirmés par un tiers. A l'inverse, les actes authentiques doivent être certifié par un officier assermenté.

La loi française modifie l'article 1317 du code civil en vue d'autoriser la certification conforme par un officier public par voie électronique semblable à une notarization aux Etats-unis.

L'obligation de faire certifier ou authentifier certains documents par une tierce personne demeure, mais peut être accomplie désormais par voie électronique et sans la présence de l'officier assermenté. La loi française précise qu'une telle confirmation peut être accomplie électroniquement si cette mesure est établie et conservée dans des conditions fixées par décret en conseil d'Etat (1).

<u>Paragraphe 3</u> : Luxembourg et Belgique

1) Luxembourg:

La loi du 14 Août 2000 sur les signatures électroniques envisage deux catégories de certificats:les certificats agrées, qui correspondent aux certificats qualifiés au sens de la directive européenne, et les autres certificats. Mais la plupart des dispositions de loi ne concernent que les certificats « agrées ».

---

(1) Décret n° 2001-272 du 30 mars 2001, j.o.numéro 77 du 31 mars 2001, p. 5070.

Qu'il soit agrée ou nom, un certificat peut être détenu par une personne physique ou morale. La loi ne comporte aucune mention explicite sur la durée de validité des certificats.

Les certificats agrées devront en particulier comporter l'indication de leurs dates d'émission et description (1).

Cependant, la délivrance des certificats agrées sera réservée aux tiers de certification accrédités, ainsi qu'a ceux qui ne sont pas accrédités, mais qui satisfont aux exigence de l'annexeII de la directive européenne.

Les tiers de certification seront surveillés par l'autorité nationale d'accréditation et de surveillance, qui sera également chargée de délivrer une accréditation à ceux d'entre eux qui en font la demande.

2) Belgique:

La loi du 09 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification traite du seul certificat qualifié qui satisfait aux exigences visées à l'annexe I de la directive européenne et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la directive européenne.

<u>Paragraphe4</u>: Allemagne et Italie

1) Allemagne :

Le certificat est la pierre angulaire de la signature électronique car il établit la relation matérielle entre le signataire et la signature. Selon la définition allemande : « il s'agit d'une attestation électronique qui attribue une clé de vérification de signature à une personne et confirme l'identité de cette personne ». (article2-9)

Le droit allemand attribue au certificat la fonction de délivrer une clé publique à un signataire, et surtout de garantir l'identité du signataire (2).

---

(1) www.senat.fr

(2) Béatrice Jaluzot, op.cit., p.2868.

La loi allemande, la directive européenne et le décret du 30 mars2001 consacrent deux catégories de certificats, le simple et le qualifié. La terminologie est ici unanime.

En ce qui concerne les relations entre la signature et le certificat , la loi allemande prévoit que la signature électronique qualifiée et fondée sur un certificat qualifié (article 2,3 a).

De même, le droit Français tout comme la directive européenne, ne fait aucune mention du lien existant entre signature et certificat. Seul le législateur allemand a adopté une position claire en matière de signature qualifiée.

Les certificats non qualifiés ne sont ni prohibés, ni réglementés par aucun des trois systèmes juridiques, ils sont donc libres de forme et de contenue. En revanche, le certificat qualifié a été minutieusement réglementé. Selon le droit allemand il consiste en la délivrance d'une clé de signature mais il est aussi le résultat d'une procédure de vérification de l'identité de ce dernier.

La loi allemande prévoit que le certificat contient une clé de signature (paragraphe 7 de l' article2) ainsi que la description des algorithmes employés (p7 de l'article 3) ce qui diverge des dispositions européennes selon lesquelles le certificat doit comporter « des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire » (annexe I, de la directive européenne et comporter la signature avancée du prestataire délivrant le certificat (Annexe I, H de la directive européenne).

2) Italie:

Selon le décret présidentiel du 1997, la signature digitale soit être produite par une clé privée dont la clé publique correspondante, préalablement certifiée par un prestataire de service de certification agrée , est encore valable .Les titulaires des certificats sont des personnes physiques . La validité de ces certificats ne peut excéder trois ans (1).

(1) www.senat.fr

En ce qui concerne les tiers de certification , les articles 8 et 9 du décret 1997, qui précisent respectivement les critères que doivent remplir les tiers de certification et les obligations qu'ils doivent respecter , sont similaires aux exigences posées par l'annexe II de la directive européenne.

<u>Paragraphe5</u> : Royaume Uni- Espagne- Danemark

1) Royaume Uni:

Le Royaume-Uni avec L'ELECTRONIC COMUNICATION ACT 2000 reprendre le même régime juridique de la directive européenne (1).

2) Espagne:

La loi éspagnole définit seulement le contenu des certificats "reconnus", c'est-à-dire de ceux que la directive européenne qualifiée de "qualifiés".
Les certificats reconnus devront répondre aux mêmes critères que ceux posés à l'annexe I de la directive européenne.

3) Danemark:

La loi du 31 mai 2000 définit les certificats d'une façon général, mais ne traite que les certificats « qualifiés ». Cette appellation sera réservée aux certificats remplissant des conditions similaires, à quelle que mots près, à celles qui figurent à l'annexe I de la directive européenne.

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

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

---

(1) voir l'annexe I de la directive européenne

CHAPITRE 2 : LES EFFETS JURIDIQUES DE LA SIGNATURE ELECTRONIQUE

La signature électronique pourra constituer la preuve en justice, c'est pourquoi il convient d'étudier, dans un premier temps, sa force probante.

Aussi, l'élément central qu'est le prestataire de service de certification pourra être mis en cause, il conviendra, dans un second temps, d'étudier son régime de responsabilité (1).

Section 1 : La force probante de la signature électronique

Il convient désormais d'analyser les questions touchant à la force probante et même à la validité des documents obtenus ou transférés par des techniques de reproduction et de communication à distance.

Paragraphe 1 : L'écrit électronique équivaut à l'écrit sur support papier dans la CNUDCI et l'Union Européenne et en Algérie.

1) La CNUDCI :

La loi type de la CNUDCI de 2001 met sur un même pied d'égalité l'écrit sur papier et l'écrit sur support électronique.

En effet, la loi dispose dans son article 1er, que le régime des contrats écrits s'applique aux contrats électroniques quant à l'expression de la volonté, à leur effet légal, à leur validité et à leur exécution… ».

De cette manière elle donne un grand rôle au juge puisqu'en cas de conflit de preuve littérale et à défaut de convention valable entre les parties ou lorsque la loi n'a pas fixé d'autre principes, le juge est tenu de déterminer par tous moyens le titre le plus vraisemblable quelqu' en soit le support.

Les actes sous seing privé ne font foi que jusqu'a preuve contraire de la sincérité des droits et obligations qu'ils constatent. L'acte sous seing privé n'à de force probante que lorsque la signature électronique est reconnue (2).

---

(1) Julien Esnault, op.cit., p. 23.
(2) www.abc.webmarkeling.com

Lorsque la signature de l'acte sous seing privé est contestée, il appartient à celui qui se prévaut de l'acte de prouver sa sincérité.

Il à noter que l'acte sous seing privé a été reconnu la même foi que l'acte authentique. Néanmoins, l'écrit électronique n'à de force probante équivalente à l'écrit sur support papier que s'il réunit toutes les conditions de forme nécessaires à sa validité. En effet, certaines obligations et conditions sont nécessaires :

1)-Obligations de l'émetteur et du destinataire :

L'émetteur s'engage à conserver le document électronique dans la forme de l'émission. Le destinataire s'engage à conserver ce document dans la forme de la réception.

2)-conditions de l'écrit électronique :

Identification de l'émetteur et du destinataire : cette première condition découle de l'obligation de l'émetteur et du destinataire de conserver le document tel qu il est.

Durée de validité.

Intégrité du message, c'est à dire qu'en aucun cas le massage ne peut être modifié.

Date et lieu de son émission ou de sa réception.

Dans l'admission de l'écrit électronique comme moyen de preuve il faut que celui ci soit établi et conservé dans des conditions de nature à en garantir l'intégrité. Par conséquent, lorsque l'écrit électronique remplit les mêmes conditions que l'écrit sur support papier et qu'il est signé afin de constater des droits et des obligations, il aura la force probante d'un acte sous seing privé et ne pourra être combattu que pour un acte authentique ou seing privé.

3) -l'acte authentique: la loi ne parle pas de document électronique en tant qu'acte authentique mais des pourparlers sont en effervescence afin de rendre l'acte authentique électronique.

Ceci n'est pas très aisé car pour l'acte authentique, la présence d'un officier public est nécessaire.

Mais une fois l'acte authentique rendu immatériel, il aura alors la même force probante que l'acte authentique matériel.

4)-En cas de conflit de preuves :

Un conflit de preuves pourrait surgir dans le cas ou les parties ont signé un écrit sur support papier et qu'il existe un écrit électronique qui le contredit, ou encore dans le cas ou deux écrits électroniques sont produits.

Le juge aura pour mission ici de régler les conflits de preuve en déterminant le titre le plus vraisemblable quelque soit le support dans la mesure où les parties n'ont pas convenu d'une clause. Il y a d'autres articles dans la loi type 2001 concernant la force probante : il s'agit de l'article 7 et l'article 9.

L'article 7 dispose que « lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données :

a)- Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données.

b)- Si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été crée ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière.

L'article 7 se fonde sur la reconnaissance des fonctions remplies par la signature dans les échanges sur papier. Afin de garantir qu'un message ne puisse se voir refuser la valeur juridique du simple fait qu'il n'a pas été authentifié de la manière voulue pour les documents sur papier, une formule générale a été retenue par cet article. Celui ci s'attache aux deux fonctions traditionnelles de la signature, à savoir l'identification de l'auteur d'un document et l'intégrité des données. Le paragraphe 1,a) précise que" cette méthode doit présenter un degré de fiabilité suffisante (1).

---

(1)Santiago, Cavanillas Mugica, Vincent Gautrais, Didier Gobert, Rosa Julia, Barcelo, Etienne Montero, Yves Poullet, op.cit., p.78.

cette condition est toutefois très relative , et sera soumise à l'appréciation souveraine du juge , car elle dépendra de l'objet pour lequel le message de données a été créé ou communiqué , compte tenu de toutes les circonstances , y compris tout accord entre l'expéditeur et le destinataire du message de données ".

L'article 7 n'établit donc pas de distinction entre les situations dans lesquelles les parties à des transactions de commerce électronique sont liées par un accord antérieur et celles dans lesquelles les parties n'avaient aucune relation contractuelle préalables. En l'absence de convention, il présente donc un intérêt non négligeable.

L'article 9 dispose que « lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence :

a) S'il existe une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été crée pour la première fois sous sa forme définitive en tant que message de données ou autre.
b) Si, Lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée.

Donc l'article 9 a pour objet d'établir l'admissibilité des messages de données en tant que moyen de preuve dans les procédures juridiques ainsi que leur valeur probante, et cela indépendamment de la présence ou non d'une signature. S'agissant de l'admissibilité, le paragraphe 1,a) prévoit que les messages de données ne devraient pas être rejetés en tant que moyens de preuve au seul motif qu'ils empruntent la forme électronique.

Tout document électronique doit donc être déclaré recevable par le juge. Les différents textes adaptés par la CNUDCI ne sont pas contraignants. Il ne s'agit pas de conventions internationales destinées à être ratifiées par les Etats. Il s'agit simplement d'une bonne source d'inspiration mise à la disposition des législateurs nationaux.

Ces textes méritent néanmoins une attention particulière dans la mesure ou ils constituent un ensemble de règles internationalement acceptables, qui permettent une certaine harmonisation et qui exercent une influence évidente sur les autorités européennes.

2) L'Union Européenne :

D'après la directive européenne du 13 décembre 1999, seules les signatures électroniques crées dans des conditions de sécurité optimale peuvent avoir la même valeur que les signatures manuscrites. En effet, cette équivalence est réservée aux signatures électroniques avancées basées sur un certificat qualifié et crées par un dispositif sécurisé de création de signature (1).

L'article 5 de la directive traite des effets juridiques de la signature électronique. Afin de reconnaître une valeur juridique à la signature électronique, cet article contient deux clauses : l'une d'assimilation et l'autre de non discrimination.

1- Les états membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et crées 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.
b) Soient recevables comme preuves en justice.

2- Les états membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées d'une signature électronique au seul motif que :

-La signature se présente sous forme électronique.

-Qu'elle ne repose pas sur un certificat qualifié.

---

(1) www.serrat.fr

-Qu’elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification.

-Qu’elle n’est pas créée par un dispositif sécurisé de création de signature.

D’un point de vue législatif, il est étonnant que l’article 5.1 commence par traiter de la force probante (point a) des signatures électroniques avancées pour ensuite envisager leur recevabilité (point b) puisque celle – ci est un préalable et une condition indispensable de leur reconnaissance juridique. De plus, notons que cette clause d’assimilation ne profit pas à l’ensemble des mécanismes de signature électronique, mais uniquement aux signatures électronique avancées (pour autant que les autres conditions soient remplies).

La clause de non discrimination (article 5.2) s’applique lorsque les conditions prévues d’article (5.1) ne sont pas remplies pour bénéficier de la clause d’assimilation. Dans ce cas les états membres doivent veiller à ce que l’effet ou la validité juridique d’une signature électronique ne soit pas contesté au seul motif que la signature se présente sous forme électronique, ou qu’elle ne repose pas sur un certificat qualifié, ou encore qu’elle ne repose pas sur un certificat délivré par un prestataire de service de certification accrédité au sens de la directive. Le principe énoncé dans cet article doit être entendu comme celui de la recevabilité des signatures électroniques.

Toutefois à défaut de répondre aux spécifications de l’article (5.1) il appartient à celui s’en prévaut de convaincre le juge de sa valeur probante (1).

La formulation de l’article 5 appelle deux commentaires:

Puisque l’article 5.1 traite de la force probante des signatures électroniques avancées, il n'était pas nécessaire de traiter dans un second temps de leur recevabilité puisque celle-ci est une condition de leur reconnaissance juridique.

---

(1) Santiago, Cavanillas Mugica, Vincent Gautrais, Didier Gobert, Rosa Julia, Barcelo, Etienne Montero, Yves Poullet, op.cit., p.87.

Il eut donc été plus clair de poser, dans un premier temps, le principe de recevabilité de toute signature électronique et de traiter, dans un second temps, de la force probante des signatures électroniques avancées. De plus, cela aurait évité de devoir traiter du problème de la recevabilité dans la clause d'assimilation (article 5.1, b), comme évoqué plus haut.

Ensuite, on peut observer qu'en pratique, l 'article 5.1 de la directive ne présente un intérêt que si les états membres, tout en respectant le principe de la liberté d'exercice de l'activité de certification, mettent un régime d'accréditation au respect des conditions prévues à l'annexe 2, ce qui suppose la mise en place d'une procédure d'octroi de l'accréditation et un contrôle préalable, sous la forme d'un audit, du respect de ces conditions.

3) L'Algérie:

L'article 323 Bis 1 du code civil dispose que « l'écrit sous forme électronique est admis en tant que preuve au même titre que l'écrit sur support papier, à la condition 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 ».

Une signature électronique sûre est la condition indispensable à la validité des contrats conclus selon des systèmes n'ayant pas recours à l'échange de documents papier. Elle est donc la clé de voûte d'un nouveau cadre juridique tant au plan communautaire que national, des transactions conclues par voie de communication électronique (commerce électronique) (1).

---

(1)Alain Bensoussan, Yves Le Roux, Cryptographie et signature électronique, édition HSP, 1999, p.78.

Le développement du commerce électronique demande l'existence d'une sécurité pour la transmission de données et les paiements en ligne. Grâce à un système de chiffrement, appliqué à l'abrégé du message transmis, la signature électronique peut être une réponse à ce besoin car elle assure plusieurs fonctions dont celles de garantir l'authenticité et l'intégrité des données, ainsi que l'identité du signataire. Or l'écrit électronique, conçu comme preuve juridique, s'appui avant tout sur la signature électronique dans le domaine du multimédia (1).

Les documents électroniques ne pourront ainsi avoir force probante que dans la mesure où s'ils s'avéreront suffisamment "fiable". C'est-à-dire qu'un document authentifié par la signature de la personne dont il émane (2).

En ce qui concerne la signature électronique en Algérie Mme fouzia Guessoum, directrice générale de SG Software, société de services informatiques, spécialisée dans la gestion électronique des documents (GEIDE) a donné un avis sur la signature et l'écrit électronique dans un séminaire tenu le lundi 2 mai 2005 à Alger, en collaboration avec le centre des techniques de l'information et de la communication CETIC) sur le thème " la capture et le stockage des documents ": «même si le document numérique a valeur probante aux yeux de la justice, nous attendons tout de même que les décrets d'application soient promulgués pour savoir exactement comment se fera l'application de cette loi»(3).

---

(1) Guenièvre Bordinat, op.cit., p.1.

(2) Lionel Bouchurberg, Internet et commerce électronique,deuxième édition 2001, p.136.

(3) www.algérie-dz.com

L'écrit électronique et la signature électronique électronique visent principalement deux objectifs. Le premier est de favoriser les échanges électroniques en donnant force probante à l'écrit électronique. Le second est de favoriser le commerce électronique en créant la notion d'acte authentique signé, non répudiable et apposable aux tiers.

Le droit d'Internet est un droit mobile. Jusqu'à aujourd'hui la preuve était fixée dans le temps, avec Internet le temps est fragmenté (1) .Ainsi deux personnes qui utilisent deux navigateurs différents (Netscape et Navigateur par exemple) verront la même chose sur leurs écrans.

Le droit de la preuve pose donc que l'écrit représente la preuve légale parfaite. C'est encore plus vrai dans le flou actuel qui sévit sur le Net. De véritables difficultés existent sur Internet, concernent la détermination exacte du moment et du lieu de l'accord, concernant l'authentification des parties ou encore la preuve du consentement lui –même; et le mode de résolution de ces problèmes a été et reste toujours l'écrit. Que ce soit par l'envoi d'un fax, d'un courrier électronique ou d'une simple lettre postale, les parties confirment ainsi leur accord. Cela leur permet, en cas d'éventuels contentieux, d'apporter au juge la preuve de ce qu'elles affirment et l'atteinte qui leur est portée.

<u>Paragraphe 2</u> : L'écrit électronique équivaut à l'écrit sur support papier en France et Etats-Unis

1) France:

En adaptant la loi portant adaptation du doit de la preuve aux technologies de l'information et relative à la signature électronique, la France a pris acte de la directive communautaire du 13 décembre 1999 dans un cadre commun pour les signatures électroniques (2).

---

(1)Michelle Jean-Baptiste, Créer et exploiter un commerce électronique, édition LITEC, 1998, p.120.

(2) Sofiane Azabi, « Le nouveau régime probatoire Français après l'adoption de la loi portant adaptation du droit de la preuve aux technologies de l'information et relatif a la signature électronique », article publié sur le site : signelec.com du 13 Mars 2000, p. 1.

La loi du 13 mars 2000 devait exprimer la modernité du droit civil français face à la nouvelle donne des échanges commerciaux électroniques.

La confrontation du droit français de la preuve aux nouvelles manifestations de l'écrit débute avec la réforme de 1980, occasion d'un examen du problème de la reconnaissance de la valeur probante d'écrit transmis à distance (télécopie) , démultipliés (photocopie) et archivés sur support photographique (microfilm) . Si ces nouvelles formes d'écrits posent à l'analyse doctrinale les mêmes défis conceptuels que ceux associés aux nouvelles technologies de l'information, il ne s'inscrivent pas dans une mouvance sociale comparable à celles ci puissamment symbolisées aujourd'hui par l'Internet. Le principe en droit français est celui du consensualisme mais il s'organise en fait autour de l'écrit, même si le contrat est valablement formé sans écrit du seul fait de l'échange des consentements des parties. La nécessité pour les parties de prouver leur contrat leur impose, le recours à un écrit.

En droit français le régime de la preuve est différent selon que l'on se trouve en matière civile ou commerciale. Ainsi pour un contrat conclu entre particuliers, la preuve sera établie selon les règles de droit civil (c'est à dire par écrit conformément à l'article 1341 du code civil).

Par contre, pour un contrat conclu entre deux commerçants, on appliquera les règles de preuves du droit commercial. Quant aux contrats dits mixtes, qui sont conclus entre un commerçant et un consommateur, les règles plus favorables du droit commercial. Il paraît donc important de dire quelques mots du régime de la preuve en droit commercial puisque c'est celui-ci qui aura vocation à s'appliquer dans la majeure partie des cas dans le cadre du commerce électronique (1).

---

(1) Julien Esnault, op.cit., p. 24.

Ce régime se résume, en fait, assez aisément par la lecture de l'article 109 du code de commerce qui pose que la preuve en matière commerciale est totalement libre :

« A l'égard des commerçants, les actes de commerce peuvent se prouver par tout moyens à moins qu'il n'en soit autrement disposé par la loi ».

Il semble donc que l'écrit ne soit plus roi en matière de preuve et à fortiori dans le cadre du commerce électronique.

La loi du 13 Mars 2000 redéfinit, dans son nouvel article 1316 du code civil la notion de preuve littérale, afin de la rendre indépendante de son support aux termes de cet article « la preuve littérale, ou preuve par écrit, résulte d'une suite de lettre, de caractère, de chiffre ou de tous autres signes ou symboles dotés d'une signification intelligible, quelque soient leur support et leurs modalités de transmission ».

L'écrit au sens traditionnel est le titre original revêtu d'une signature manuscrite et matérialisé dans un document papier. Un écrit est exigé pour toute convention d'ont l'objet vaut plus de 800 euros. De plus, quand un écrit a été rédigé, on ne peut apporter la preuve contraire que par un autre écrit.

La signature remplit deux fonctions juridiques essentielles : identification de l'auteur et manifestation de sa volonté, adhésion personnelle du signataire au contenu du document.

L'article 1341 du code civil affirme l'exigence d'un écrit pour faire la preuve d'un acte juridique.

Il reçoit plusieurs exceptions dont notamment celles énoncées aux articles 1347 et 1348 du code civil.

Le premier de ces textes, l'article 1347 du code civil, fait état des commencements de preuve par écrit.

La seconde possibilité évoquée par le CNCT, l'article 1348, prévoie une nouvelle exception au principe de la preuve littérale lorsque le titre est établi et conservé sous forme électronique, eut présenté l'avantage d'introduire cette forme dans le droit civil, mais l'inconvénient de le faire d'une manière dédaigneuse car il aurait été pour le moins paradoxal de vouloir consacrer une nouvelle notion par le biais d'une

simple exception. Il en eût résulté que la loi ne considère pas le titre électronique comme un acte écrit sous seing privé.

Cette définition assez abstraite de l'écrit, comme mode de preuve littérale permet de dégager clairement si les écrits utilisés répondent aux caractéristiques données.

On confirme la synonymie du littéral et de l'écrit. Il s'agit d'une suite de signes ou symboles, de lettres, de chiffres destinés à être communiqués et à être compris (1).

En ce qui concerne l'écrit électronique, la loi française apporte des réponses précises à la manière dont ces principes doivent s'appliquer.

Aux termes de l'article 1316 – 1 du code civil « l'écrit sous forme électronique est admis en matière de preuve au même titre que l'écrit sur support papier , sous réserve que puisse être dument identifiée la personne dont il émane et qu'il soit établie et conservé dans des conditions de nature à en garantir l'intégrité ».

Cet article met sur un pied d'égalité le document numérique et le document papier. Ce texte permet à la loi de poursuivre l'œuvre amorcée par la jurisprudence qui avait déjà dissocié l'écrit de son support. Afin d'assurer la sécurité juridique du document électronique, la loi exige cependant qu'il répondre à une double condition. Un document électronique ne pourra être admit à titre de preuve qu'a conditions que soit identifiée la personne dont il l'émane et qu'il soit établit et conservé dans des conditions de nature à en garantir l'intégrité.

Dés qu'un document électronique répond à cette double exigence, non seulement il est admis comme preuve, mais il revêt la même force probante qu'un acte sous seing privé.

---

(1) Sofiane Azabi, op.cit., p.2.

Ces critères avaient déjà été dégagés par la jurisprudence dans des termes pratiquement similaires par la chambre commerciale de la cour de cassation dans un arrêt rendu le 02 Décembre 1997, la cour de cassation avait en effet jugé qu'un écrit pouvait être établi et conservé sur tout support y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées.

En cas de conflit de preuve littérale, si la question n'est pas réglée par un texte de loi et à défaut d'accord entre les parties, il appartiendra aux juges, selon l'article 1316-2 de régler ce conflit en déterminant par tout moyens le titre le plus vraisemblable, quel qu'en soit le support.

Confirmant à nouveau la jurisprudence, l'article 1316-2 reconnaît d'une part la validité des conventions sur la preuve et a pour conséquence d'autre part de supprimer toute hiérarchie entre la preuve sous forme électronique et la preuve littérale traditionnelle.

Il reste que pour l'heure, grâce au nouveau texte, de nombreuses conventions pourront être conclues sans que les parties se déplacent, ni ne s'envoient de courrier manuscrit, services, ventes de bien meubles et immeubles , corporels ou incorporels (et même certaines sûretés, car l'article 1326 est spécialement réaménage) le champ et très large, du moins, semble très large.

En ce qui concerne les limites de l'assimilation de l'écrit électronique a l'écrit papier, le droit Français accueille un double aspect des règles de preuves en les distribuant, selon leur fonction, entre les lois de fond et les lois de procédure sont des lois de fond celles qui définissent le fait de prouver, celles qui déterminent les moyens de preuve admissibles selon la matière du litige.

Celles enfin qui fixent la force probante de certains procédés de preuve. Au contraire, les lois qui gouvernent l'administration de la preuve en justice ressortent de la procédure. La loi du 13 Mars 2000 est une loi de fond et se borne à confier au document électronique une valeur probante susceptible d'être apporté et retenu en justice.

En droit français, l'écrit à soit une valeur probatoire soit une fonction solennelle tendant à protéger le consentement des parties. Dans le dernier cas l'écrit est exigé ad validitem, pou assurer la validité juridique de l'acte. Or aucune mention de cette fonction n'est faite dans la nouvelle loi,et pour cause, cette fonction à été énergiquement écartée par le garde des seaux lors des discusions et du vote du projet .la loi n'introduit l'écrit électronique au même rang que le papier que lorsque la forme n'est requise qu'a titre probatoire de sorte que , compte tenu de ses termes et de la place des nouvelles dispositions , il ne pourra pas être tenu pour un véritable écrit lorsque la forme est requise pour la validité même de l'acte . Ensuite, le législateur a inséré l'article 1316-3 dans le code civil attribuant à l'écrit électronique la même force probante qu'a l'acte sous seing privé (1).

L'arrête du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèderont à leur évaluation précise les règles pour reconnaître la qualification d'un prestataire de certification électronique. Cette qualification est importante car elle permet la présomption de la fiabilité d'une signature électronique.

L'arrêté du 26 juillet 2004 complète le décret du 30 Mars 2001 pris en application de l'article 1316 – 4 du code civil. Ainsi, le comité français d'accréditation (cofrac) et les organismes signataires d'un accord européen sont chargés d'accréditer, pour une durée de deux ans, les organismes qui procéderont à l'évaluation des prestataires.

---

(1) Julien Esnault, op.cit., p. 30.

Le nouvel article 288-1 du nouveau code de procédure civile traite de la signature électronique et dispose « lorsque la signature électronique bénéficie d'une présomption de fiabilité, il appartient au juge de dire si les éléments dont il dispose justifient le renversement de cette présomption ».

Cette règle de procédure est, à première vue, le prolongement de la présomption de fiabilité de l'article 1316- 4 du code civil, qui est une présomption simple, la signature qui est nécessaire à la perfection de l'instrumentum a pour unique résultat d'en faire un acte sous seing privée semblable à un acte sur support papier, cette présomption de fiabilité ne porte que sur la signature électronique sécurisée. En effet , si la signature électronique ne bénéficie pas de la présomption d'équivalence avec l'écrit papier , elle peut constituer un commencement de preuve par écrit qui pourra , dés lors , être complété par tous moyens.

Avec la signature électronique, les professionnels peuvent en toute tranquillité transmettre leurs factures, bon de commande. Ils peuvent également effectuer leurs déclarations fiscales et sociales (1).

La signature électronique permet aux entreprises de déposer leur comptes en ligne auprès du greffe du tribunal de commerce, d'accomplir certaines formalités en ligne auprès de celui-à, et également de consulter et d'obtenir en ligne des documents sécurisés.

Il y a différent type de signature électronique, mais les plus utilisées sont :

- La cryptographie asymétrique.
- La cryptographie symétrique.

---

(1) Le service juridique de la fédération des entreprises internationales de la mécanique et de l'électricité, Rev. Le MOCI. N°1606 du 10 juin 2003:" signature électronique, a la recherche de la confiance dans l'économie numérique", p .77.

Mais la question qui se pose : qu'est ce que la cryptographie ?

La cryptographie est une technologie qui permet de chiffrer les messages et de les rendre illisibles par un tiers. Elle est l'un des moyens essentiels pour sécuriser les échanges sur Internet (1).

Afin de garder un contrôle étroit sur l'utilisation de ces technologies, l'état français dispose d'une réglementation complexe et restrictive. Néanmoins, dans le cadre de son programme de promotion de la société de l'information, il a entamé en janvier 1999 une libéralisation progressive des technologies de cryptage. En attendant un régime de liberté totale, la première étape a consisté à accorder la liberté d'utilisation des moyens de cryptologie jusqu'à 128 Bits.

La cryptographie est l'art de transformer des informations lisibles (texte) en des informations que seules les personnes autorisées peuvent lire. Au cours de ce processus, l'information est codée (chiffrée) de façon à ce que seul le destinataire puisse lire ou altérer le message. Il peut être intercepté mais n'est intelligible que pour la personne qui est capable de le décoder (déchiffrer) (2).

Le chiffrement et le déchiffrement nécessitent une formule mathématique (ou algorithme) pour convertir les données lisibles en un format codé et une clé. Une clé est un nombre unique, combiné avec du texte pour produire un message chiffré ou une signature électronique. Pour la définition de la clé : une clé est une valeur numérique qui fait partie de l'algorithme de chiffrement. Il s'agit d'une suite de caractères utilisés pour coder et décoder un dossier. La clé est utilisée pour chiffrer et déchiffrer un message.

---

(1)Nicolas Macarez-Fançois Lesle, Que sais je"commerce électronique, 1er édition 2001, p. 115.

(2) www.signature électronique.be

Pour la cryptographie de clés symétriques, la même clé et utilisée pour chiffrer et déchiffrer le message. Pour la cryptographie clé publique la clé publique est utilisée pour chiffrer le message, alors que la clé privée est utilisée pour déchiffrer le message.

Les signatures électroniques utilisent la cryptographie clé publique. Deux clé sont utilisées pour encrypter et décrypter le message.

Une signature électronique est créée en utilisant la clé privée d'une personne.

Le destinataire vérifie la signature en utilisant la clé publique de l'expéditeur.

Dans un système de cryptographie clé publique, deux clés sont nécessaires pour que les deux parties puissent échanger des données de façon sure : une clé publique et une clé privée. L'une est utilisée pour chiffrer le message et seule l'autre clé de la partie permet de le déchiffrer.

Bien que les deux clés de la paire soient liées de façon mathématique, il est impossible de trouver une clé a partir de l'autre. La clé privée ne peut donc être reproduite ou falsifiée à partir de la clé publique correspondante. Il est donc possible de distribuer sa clé publique, mais il est essentiel de garder sa clé privée secrète. La clé publique est donc utilisée pour vérifier un message signé avec la clé privée ou pour chiffrer des messages qui ne pourront être déchiffrés qu'en utilisant la clé privée. Si quelqu'un veut envoyer un message chiffré, il chiffre le message avec la clé publique.

En France, la cryptographie est réglementée par de nombreux textes, mais deux décrets jouent un rôle majeur:

Le décret N° 99-1999 du 17 Mars1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.

Le décret N° 99-2000 du17 Mars1999 définissent les catégories de moyens et le la prestations de cryptologie dispensées de toute formalité préalable (1).

2) Etats-Unis :

Le système américain se caractérise par la volonté de trouver un équilibre entre la liberté de choix du marché et une législation minimale assurant le développement du commerce électronique, en protégeant le consommateur et le citoyen. Les états jouissant d'une indépendance législative certaine, le risque majeur est de voir des incompatibilités juridiques entre états mettre en danger les objectifs fixés conscient du risque, la « confiance nationale des commissaires à l'uniformisation des lois des états » a établi une proposition de loi applicable sur les transactions électronique, nommée « l'uniform transaction act » que les états peuvent adopter (UTA).

L'esprit de l'UTA est en fait très proche de celui de la directive européenne en ce qui concerne la manière dont il apporte la signature électronique dans le droit local.

Dans ses termes et son applicabilité, l'acte est extrêmement pratique et indique :

Qu'il n'est pas applicable si la loi locale prévoit des dispositions contraires ou différentes.

Que la signature électronique est recevable et qu'elle ne peut être refusée au seul titre qu'elle est électronique.

Que la convention de preuve entre les parties reste libre et l'acte n'impose rien dans ce domaine.

Que si la loi demande un écrit, un écrit numérique satisfait la requête.

Que si la loi demande une signature, la signature électronique satisfaite la requête.

La manière dont les documents numériques peuvent se substituer aux documents papier est référencée dans les lois.

---

(1) Arnaud –Fausse, La signature électronique"transactions et confiance sur Internet", édition 2001, p. 81.

Que la signature électronique n’a pas de valeur intrinsèque mais dépend du contexte dans lequel elle est effectuée.

Que l’imputabilité à une personne peut être démontrée par tout moyen, notamment par la démonstration de l’efficacité des mesures de sécurité (aucune mesure technique explicite n'est citée).

La résolution de problèmes transactionnels, (les responsabilités et les réactions des parties encas d’erreurs détectées dans les transactions).

Que les actes authentiques peuvent être recouvert de la signature électronique de l’officier autorisé.

Que la signature peut être effectuée par des systèmes automatiques (serveurs de transactions).

Les conditions opératoires permettant d’établir qu’un document électronique a été émis, reçu et commercialement cédé (spécifications d’événements techniques définissant l'entré d’un message dans un système d’information).

Les conditions d’archivage des données électroniques (opératoires, sécuritaires).

En ce qui concerne la loi de l’UTA: trois fonctions de la signature se retrouvent clairement dans cette loi, la fonction d’intégrité est directement consacrée dans la définition de la signature digitale. Les fonctions d’identification et de manifestation de la volonté sont envisagées par le biais des présomptions, on ne peut toutefois pas parler véritablement d’une approche fonctionnelle puisque le seul mécanisme visé par cette loi est celui de la signature numérique. Il en résulte que d’autres mécanismes de signature électronique ne pourront bénéficier, même s’ils remplissent ces trois fonctions, des présomptions de cette loi et de l’équivalence juridique à la signature manuscrite. Toutefois et même si la loi de l’UTA ne se prononce pas expressément sur la recevabilité de l’ensemble des signatures électroniques, on devrait pouvoir considérer que tel est quand même le cas. Pour le reste le juge resterait libre d’en apprécier la valeur probante, à défaut pour bénéficier des présomptions de la loi.

Il apparaît raisonnable qu' on ne reconnaisse pas automatiquement force probante à tous les mécanismes de signature électronique s'il existe un doute sur leur fiabilité ou si leur utilisation n'est pas faite dans un contexte sécurisé ,tel que celui retenu par cette loi .

En plus, la coexistence des règles de Common Law avec l'utilisation grandissante des documents informatiques a obligé les pays soumis à ses règles à adapter leur législation. Ainsi une grande majorité des états fédéraux des états unis ont modifié leurs règles de preuves dans les années 75 pour autoriser la recevabilité des documents informatiques.

Certains états vont même jusqu'à admettre expressément la signature électronique.

c'est le cas de l'état de l'Utah ,qui ,en 1995,se dote du Utah digital signature Act qui prévoit qu'un document informatisé revêtu d'une signature électronique sera valable au même titre qu'un document écrit traditionnel .

<u>Paragraphe 3</u> : **L'écrit électronique équivaut à l'écrit sur support papier en Luxembourg et Belgique.**

1) **Luxembourg** :

Il figure dans la partie de la loi du 14 août 2000 qui est consacrée autorités de certification. Seules les signatures électroniques crées dans des conditions de sécurité optimales auront la même valeur que la signature manuscrite (1).

L'article 17 de loi prévoit en effet : "

1 Qu'une signature électronique crée par un dispositif de création de signature que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat qualifié , constitue une signature au sens de l'article 1322 – 1 du code civil.

2 Une signature électronique ne peut être rejetée par le juge au seul motif qu'elle se présente sous forme électronique, qu'elle ne repose pas sur un certificat qualifié ".

---

(1) www.senat.fr

Le premier paragraphe constitue la clause d'assimilation au sens de la directive européenne. Eu égard aux niveaux de sécurité et de la fiabilité résultant du respect des conditions stipulées dans ce paragraphe, une telle signature doit être considérée comme équivalente à une signature manuscrite sans qu'un juge ne puisse remettre en cause sa valeur probante intrinsèque, ce qui, bien entendu, n'interdit pas à celui auquel elle est opposée de la contester à la même manière qu'une signature manuscrite. le raisonnement ne sera toutefois tenable que si l'on considère qu'un certificat qualifié est un certificat émis par une autorité de certification qui a été préalablement agrée dans le cadre d'une procédure d'accréditation , ce qui n'apparaît pas clairement dans le texte (1).

Le deuxième paragraphe consacre la clause de non-discrimination.

Si une signature électronique ne satisfait pas aux conditions prévues dans le paragraphe 1, elle ne bénéficie pas de l'équivalence automatique de la signature manuscrite, mais elle ne peut être rejetée par le juge pour cette seule raison. Il appartiendra à la personne qui s'en prévaut d'apporter la preuve de la fiabilité de la technique utilisée afin d'établir que la signature répond aux critères posés par l'article 1322-1 du code civil. A défaut, l'acte auquel elle est attachée pourrait toujours servir de commencement de preuve par écrit ou d'indice à l'appui d'une preuve par présomption. On peut se demander si ce paragraphe 2 de l'article 17 n'est pas redondant avec l'article 5 qui affirme déjà le principe de la recevabilité des signatures électroniques.

---

(1) Santiago, Cavanillas Mugica, Vincent Gautrais, Didier Gobert, Rosa Julia, Barcelo, Etienne Montero, Yves Poullet, op.cit., p.89.

2) Belgique :

La loi du 9 juillet 2001 qui fixe certaines règles relatives aux services de certification en vue de l'utilisation des signatures électroniques reconnaît à certaines signatures électroniques crées dans des conditions de sécurité optimales la même force probante qu'a une signature manuscrite.

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

Cette catégorie de signatures électroniques avancées bénéficierait d'une assimilation automatique à une signature manuscrite. Leur valeur probante s'imposerait au juge. En revanche, la valeur des autres signatures électroniques continuerait a être librement appréciée par le juge. Il convient par ailleurs de rappeler, que en matière civile , l'article 1341 du code civil prévoit qu'il « il doit être passé acte devant notaire ou sous signature privée , de toutes choses excédent une somme ou une valeurs de 1500 F» (c'est à dire f FR). Par conséquent, le juge civil est en mesure de rejeter un document au seul motif qu'il est signé électronique.

<u>Paragraphe 4</u> : L'écrit électronique équivaut à l'écrit sur support papier en Allemagne et Italie

1) Allemagne:

La loi fédérale (SIG G) du 16 mai 2001 ne contient aucune disposition explicite sur la recevabilité en justice et sur la valeur probante de la signature digitale. Elle ne remet pas non plus en cause le principe selon lequel le juge apprécie librement la force probante des éléments qui lui sont soumis (1).

---

(1) www.senat.fr

Le code de procédure civile reconnaît cinq moyens de preuve, parmi les quels « l'observation ». Or la jurisprudence admet depuis plusieurs années que l'observation ne se limite pas à l'observation visuelle et qu'elle peut s'appliquer à des document informatiques .Comme le juge apprécie librement la valeur probante des éléments qui lui ont soumis et que la loi garantit la fiabilité des signatures digitales parcequ'elles répondent aux critères qu'elle même définit et que l'ordonnance précise, il parait probable que les signatures digitales seront reconnues comme moyens de preuves , sauf dans les cas ou la loi exige une signature manuscrite .

Le législateur allemand a souhaité pouvoir faire un bien de la mise en œuvre de la loi avant de reconnaître une équivalence entre la signature digitale et la signature manuscrite, conformément à l'article 5 de la directive (1). Cependant, le ministre de la justice a déjà publié une note dans laquelle il propose que, pour certains actes juridiques requérant une signature manuscrite, l'équivalence soit reconnue.

2) Italie:

La loi italienne (dite loi bassanini) s'est prononcée sur la valeur probante à accorder à un document signé digitalement. En effet, la section 5 de cette loi dispose qu'un document électronique signé avec une signature digitale conformément aux prescriptions du décret bénéficie de la même force que l'acte sous seing privé visé à l'article 2702 du code civil italien.

---

(1) La directive européenne N° 1999/931 C/E, sur un code communautaire pour les signatures électroniques, caz.pal.29/31octobre 2000, p. 1842

La section 04 prévoit le même type d'assimilation pour le concept d'écrit puisqu'il dispose que les documents informatiques qui respectent les prescriptions du décret doivent être considérées comme rencontrant les exigences légales en matière d'écrit. Dans ce contexte, on comprend que législateur Italien ait juge superflu de donner une définition fonctionnelle abstraite de la signature, cela signifie également que le régime privilégié accordé à la signature digitale ne bénéficie pas aux autres mécanismes de signatures électroniques actuelles ou futures (1).

Dans certaines conditions, définies par le décret N°531 du 10 Novembre 1997, la signature digitale à la même valeur que la signature manuelle et peut également remplacer un sceau, un poinçon, un tampon, ainsi que n'importe quel autre signe ou marque. Ce texte prévoit que tout, comme la signature manuscrite, la signature digitale peut être authentifiée par un officier ministériel : celui –ci après vérification de l'identité de l'intéressé et de la validité de la clé utilisée, atteste que la signature électronique a été opposée en sa présence par son titulaire .

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

<u>Paragraphe 5 :</u> L'écrit électronique équivaut à l'écrit sur support papier au Royaume Unis, Espagne, Danemark

1) Royaume-Uni:

L'article 07 de la loi 2000 sur les moyens électroniques de communication indique que:

" Dans tout procès, une signature électronique incorporée ou logiquement associée à un message électronique donné, ainsi que la certification d'une telle signature, sont toutes les deux recevables comme preuves de tout élément relatif à l'authenticité ou à l'intégrité du message".

---

(1) Santiago, Cavanillas Mugica, Vincent Gautrais, Didier Gobert, Rosa Julia, Barcelo, Etienne Montero, Yves Poullet, " op.cit., p.84.

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

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

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

2) Espagne :

La loi espagnole (59/2003) reprenne les dispositions de la directive européenne.elle prévoit en effet l'équivalence de la signature manuscrite et de la signature électronique « avancée », dans la mesure ou elle se fonde sur un certificat qualifié et ou elle a été crée par un dispositif sécurité.

Le non rejet a priori de la valeur probante des autres signatures électroniques.

En conclusion , les lois Belge , Espagnol et Luxembourgeois considèrent comme équivalentes aux signatures manuscrites les signatures électroniques créées dans des conditions de sécurité optimales , c'est à dire les signatures électroniques « avancées » qui, de plus sont associées à un certificat particulièrement fiable et sont crées par un dispositif sécurisé . En revanche, elles ne reconnaissent aucun effet juridique particulier aux autres signatures électroniques. Cependant, les lois espagnoles et luxembourgeoises précisent explicitement, tout comme la directive, qu'elles seront recevables en justice.

3) Danemark:

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

Elle ne remet pas non plus en cause le principe selon lequel les juges apprécient librement la valeur probante des éléments qui leur sont soumis (1).

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

Section 2: La responsabilité des prestataires de services de certification électronique

Le prestataire de services de certification, est défini par les textes européens et français comme toute personne physique et morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques (2).

Le prestataire de service certification (PSC) a notamment pour mission de collecter des informations relatives et l'identité et à la qualité de l'émetteur d'un message et d'émettre un certificat garantissant au destinataire le lien entre le message, la signature qui lui est présentée et l'identité de l'émetteur. Le prestataire de service de certification est donc un acteur fondamental de la confiance dans le domaine de la signature électronique.

---

(1) www.senat.fr

(2) Isabelle Renard et Isabelle Védrines, "Le point sur la responsabilité des prestataires de services de certification", article publié sur le site:www.legalbiznext.com 2002, p.1.

Les conditions précises dans lesquelles ce dernier peut voir sa responsabilité engagée restent cependant à ce jour délicates à cerner.

<u>Paragraphe 1</u> : La responsabilité des prestataires de services de certification électronique dans la CNUDCI et l'Union Européenne et l'Algérie

1) La CNUDCI:

L'article 9 dans son alinéa (a) de la loi type CNUDCI sur les signatures électroniques 2001 énonce la règle fondamentale selon laquelle un prestataire de service de certification devrait se conformer à ses déclarations et à ses engagements tel qu'exprimés, par exemple, dans une déclaration de pratiques de certification ou dans tout autre type de déclaration de pratique générale .L'alinéa(c) définit le teneur et les effets essentiels de tout certificat en vertu de la loi type. Il convient de noter que s'il s'agit de signatures numériques il doit en outre être possible de vérifier le lien du signataire avec clef publique ainsi qu'avec la clef privée. L'alinéa (d) énumère les éléments additionnels qui doivent être inclus dans le certificat.

L'alinéa (e) n'a pas pour objet de s'appliquer à des certificats tels que des certificats d'opérations, qui sont des certificats ponctuels,ou à des certificats à faible coût portant sur des applications à faible risque, qui pourraient ne pas être sujets à révocation .(1)

On peut considérer qu'il est raisonnable d'attendre de tout prestataire de service de certification, et non seulement de ceux qui émettent des certificats de « grande valeurs », qu'il s'acquitte des devoirs et des obligations prévus à l'article 9.

---

(1) www.unictral.org

Toutefois, la loi type n'exige pas d'un signataire ou d'un prestataire de services de certification un niveau de fiabilité sans rapport raisonnable avec les fins pour lesquelles la signature électronique ou le certificat sont utilisés. La loi type privilégie donc une solution qui lié les obligations énoncées dans les articles 8 (1) et 9 à la production de signatures électroniques ayant une valeur juridique.

---

(1) L'article 8 : Normes de conduite du signataire:

1- Lorsque des données afférentes à la création de signature peuvent être utilisées pour créer une signature ayant des effets juridiques, chaque signataire :

a) Prend des dispositions raisonnables pour éviter toute utilisation non autorisée de ses données afférentes à la création de signature.

b) Sans retard injustifié, utilise les moyens fournis par le prestataire de services de certification conformément à l'article 9 de la présente loi, ou fait d'une autre manière des efforts raisonnables, pour aviser toute personne dont il peut raisonnablement penser qu'elle se fie la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique :

j) Il sait que les données afférentes à la création de signature ont été comprises, ou il estime, au regard des circonstances connues de lui , qu'il y a un risque important que les données afférentes à la création de signature aient été compromises.

c) Prend , lorsqu'un certificat est utilisé pour étayer la signature électronique des dispositions raisonnables pour assurer que toute les déclarations essentielles qu'il fait concernant certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes.

2-Un signataire assume les conséquences de tout manquement aux exigences.

En limitant le champ d'application de l'article 9 aux cas dans lesquels les services de certification servent à étayer une signature électronique qui peut être utilisée pour produire des effets juridiques en tant que signature, la loi type ne vise pas à créer de nouveau types d'effets juridiques pour les signatures.

Le paragraphe 2 de l'article 9 laisse à la législation nationale le soin de déterminer les conséquences juridiques du non respect des exigences du paragraphe sous réserve des règles applicables du droit national, le paragraphe 2 n'est pas destiné par ses auteurs à être interprété comme une règle de responsabilité objective sans faute. Il n'a pas été prévu que ce paragraphe ait pour effet d'exclure la possibilité, pour le prestataire de services de certification, de prouver, par exemple, l'absence de faute ou de faute secondaire.

Les premières versions de l'article 9 contenaient un paragraphe supplémentaire, qui traitait des conséquences de la responsabilité énoncées au paragraphe 2, lors de l'élaboration de la loi type, il a été observé qu'une disposition unique s'inspirant du paragraphe 2 ne suffirait pas à traiter la question de la responsabilité des prestataires de service de certification.Le paragraphe 2 énonce un principe approprié applicable aux signatures,mais il peut n'être pas suffisant pour couvrir les activités professionnelles et commerciales visées par l'article 9 . L'une des façons possibles de pallier cette insuffisance aurait été d'énumérer dans le texte de la loi type les facteurs à prendre en compte pour évaluer toute préjudice résultant d'un non respect par le prestataire de service de certification des exigences du paragraphe1.

Pour évaluer la responsabilité du prestataire de service de certification, il faudrait notamment prendre en compte les facteurs suivants :

A) Le coût d'obtention du certificat,B) La nature de l'information certifiée,C) L'existence et l'ampleur de toute restriction aux fins pour lesquelles le certificat peut être utile,D) L'existence de toute déclaration limitant le champ d'application ou l'étendue de la responsabilité du prestataire de service de certification, et E) Toute conduite fautive de la partie se fiant à la signature.

Lors de l'élaboration de la loi type, il a été généralement convenu que, pour déterminer le préjudice pouvant donner lieu à indemnisation, il faudrait tenir compte des règles de limitation de la responsabilité dans l'état ou le PSC était établi ou dans tout autre état dont les lois s'appliqueraient en vertu de la règle de conflit de lois pertinente.

2) L'Union Européenne :

Si la fourniture de services de certification ne peut être soumise à une autorisation préalable, et peut être assurée par toute personne physique ou morale, les états membres doivent cependant instaurer un système de contrôle des tires de certification. La directive européenne du 13 décembre 1999 prévoit par ailleurs que les Etats membres puissent, pour améliorer le niveau du service de certification fourni, instaurer un système d'accréditation (1).

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

« Les prestataires de services de certification doivent :

a) Faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification.
b) Assurer le fonctionnement d'un service d'annuaire rapide et sur et d'un service de révocation sur et immédiat.
c) Veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision.
d) Vérifier, par des moyens appropriés et conformes au droit national, l'identité et le cas échéant , les qualités spécifiques de la personne à la quelle un certificat qualifié est délivré.

---

(1) www.senat.fr

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

f) Utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument.

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

h) Disposer des ressources financières suffisantes pour fonctionner conformément aux exigence prévues par la présente directive, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée.

i) Enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier, pour pouvoir fournir une preuve de la certification en justice.

Ces enregistrements peuvent être effectués par des moyens électroniques.

g) Ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le PSC a fourni des services de gestion de clés.

k) avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats y compris des limites imposées à leur utilisation de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges».

Cette information qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible.

Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat.

Utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable, de sorte que :

Seules les personne autorisées puissent introduire et modifier des données.

L'information puisse être contrôlée quant à son authenticité.

Les certificats ne soient disponibles au public pour des recherches que dans les cas ou le titulaire du certificat à donner son consentement, et toute modification technique mettant en péril ces exigences de sécurité soit apparentes pour l'opérateur.

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

La directive met en place un régime spécifié de responsabilité pour les prestataires de services de certification afin d'assumer un niveau de confiance suffisant aux yeux des utilisateurs (1).

---

1) www.awt.be

Ce régime spécifique de responsabilité ne concerne cependant que les prestataires qui délivrent au public des certificats qualifiés, ou qui garantissent publiquement de tels certificats (l'article 6 de la directive européenne).

Les prestataires qui émettent des certificats ordinaires tombent sous le coup du régime du droit commun de la responsabilité .Concernant les obligations à la charge des prestataires de services de certification émettent des certificats qualifiés ou qui garantissent publiquement de tel certificats, ils peuvent être classés en deux catégories .

1) Les obligations conçernant l'objet de l'activité: Trois types d'obligations spécifiques peuvent être ici identifiées:

L'exactitude des informations fournies dans le certificat à la date de sa délivrance (pas d'obligation de contrôle permanent des obligations contenus dans le certificat).

La vérification de la détention et de la complémentarité des données afférentes à la création de signature (article 6, 1, c).

Or, cette obligation est fondamentale et devrait, peser sur tout PSC qui offre au public le niveau de certification voulu par la directive.

En effet, en émettant un certificat, le prestataire confirme le lien entre une personne et sa clé publique. La certification demeure vide de sens si, certifiant ce lien, le PSC omet de vérifier la complémentarité des clés.

Le dispositif de certification n'est, comme son nom l'indique, qu'un moyen de vérification.

L'assurance que doit avoir le destinataire d'un message signé électroniquement porte sur la garantie que la signature électronique qu'il entend vérifier émane bien du signataire. Il ne peut avoir cette garantie que, notamment, par la vérification du lien entre le titulaire et sa clé publique, la clé privée devant, par nature demeurer secrète.

La révocation des certificats, notamment du point de vue de la mise à disposition des utilisateurs d'un service de révocation sur et immédiat en veillant à ce que la date et l'heure du certificat puissent être déterminées avec précision.

Pour de multiples raison, il se pourrait que la confidentialité des données afférentes à la création de signature soit compromise ou que le titulaire du certificat craigne qu'il en soit ainsi , c'est pour parer à cette éventualité que la directive impose à tout PSC délivrant des certificats , d'assurer le fonctionnement d'un service de révocation sur et immédiat et de veiller à ce que la date et l'heure de révocation d'un certificat puissent être déterminés avec précision (annexe II,c et à).

La procédure de révocation vise donc à mettre fin à un certificat avant son terme. Par conséquent, le titulaire ne peut plus utiliser les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature certifiées dans le certificat révoqué pour générer une signature électronique. La responsabilité ne pourrait être engagée si le titulaire contrevenait à cette obligation.

2) Les obligations tenant au fonctionnement du mécanisme de certification : Elles prennent la forme de garanties que doit obligatoirement présenter le tiers certificateur. Elles concernent notamment les aspects suivants :

Sécurité et fiabilité : le PSC doit utiliser des systèmes et produits fiables (annexe II, p). Concernant les certificats, le PSC doit prendre les mesures nécessaires contre leur contrefaçon (annexe II, g). Pour cela, il doit notamment utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que :

Seules les personnes autorisées puissent introduire et modifier les données. L'information puisse être contrôlée quant à son authenticité.

Les certificats ne soient disponibles au public pour des recherches que dans les cas ou le titulaire du certificat a donné son consentement.

Toute modification technique mettant en péril cas exigences de sécurité soit apparente pour l'opérateur (annexe II, point 1).

Lorsqu'il génère les données afférentes à la création de signature, le PSC doit garantir la confidentialité au cours de ce processus, une fois ces données crées, il ne peut évidemment ni les stocker, ni les copier (annexe II, g, j).

Enfin, le PSC doit posséder l'expertise nécessaire pour assurer ses activités de certification, à cette fin, il emploie du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier des connaissances en gestion et en technologie des signatures électroniques ainsi, qu'une bonne pratique des procédures de sécurité appropriées (annexe II, E).

3) Garanties d'information: L'objectif de la directive est de renforcer la confiance et de promouvoir l'utilisation de la signature électronique avancées .l'information correcte de l'utilisateur des services contribue à la réalisation de cet objectif. Le PSC a donc l'obligation de procurer toute information nécessaire à l'utilisation correcte et sure de ses services. Ces informations doivent être fournies par un moyen de communication durable ou sur tout support durable .On vise par ces termes de nouvelles formes de communications susceptibles de remplacer l'écrit traditionnel, ces nouvelles formes de communication peuvent valablement se substituer à un écrit pourvu que l'instrument utilisé présente de garanties de fiabilité suffisantes ,et que son destinataire puisse prendre connaissance sous difficulté des informations ainsi diffusées , la proposition de directive concernant la commercialisation à distance de services financiers auprès des consommateurs définit la notion de support durable comme tout instrument au consommateur de conserver des informations, sans qu'il soit tenu de procéder lui même à l'enregistrement de ces informations, sont notamment des supports durables au sens de cette directive les disquettes informatiques , les C D-ROM , ainsi que le disque dur de l'ordinateur du consommateur stockant des courriers électroniques .

Par ailleur la proposition de directive précitée insiste sur le fait que les données stockées sur support durable doivent être accessible, c'est a dire que leur destinataire doit être en mesure d'en prendre connaissance aisément et de les conserver.

4) Garanties financières : Les PSC doit posséder des garanties financières suffisantes pour exercer ses activités et, le cas échéant indemniser les utilisateurs ayant subi un dommage suite à l'inexécution des obligations qui lui sont imposées par ou en vertu de la directive, a cet effet, il devrait ce couvrir par une assurance appropriée.

5) Garanties d'interopérabilité : Enfin comme l'indique la Commission Européenne dans sa communication du 08 octobre 1997 et dans le considérant N°05 de la directive, l'interopérabilité des différents systèmes et applications de signature électronique sécurisée est absolument nécessaire afin d'assurer que celles –ci puissent être mises en oeuvre en europe et en dehors de l'Europe.

6) protection des données a caractère personnel : Le PSC qui est chargé d'établir un certificat doit être en mesure de vérifier de manière certaine et non équivoque le candidat titulaire. A cette fin, il est amené à collecter diverses informations sur les candidats. La directive impose aux états membres de veiller à ce qu'un PSC ne puisse recueillir de données personnelles que directement auprès de la personne concernée ou avec son consentement explicite et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat (article 8.2).

Le candidat titulaire n'étant pas légalement obligé ou ne désirant pas communiquer son identité, peut choisir un pseudonyme qui lui permettra de sauvegarder son anonymat.

Le régimes de responsabilité établi par la directive tente de respecter un équilibre entre les intérêts des PSC et des utilisateurs de certificat afin que le niveau de certification mis en place présente un degré de fiabilité et, par la même, de crédibilité, sans qu'il n'entrave pour autant le commerce électronique.

Le PSC peut toute fois limiter sa responsabilité. Deux types de clauses relatives à la responsabilité peuvent figurer sur le certificat qualifié.

Le prestataire peut tout d'abord fixer des limites à l'utilisation du certificat. Dans cette hypothèse, il ne doit pas être tenu responsable du préjudice résultant de l'usage abusive de certificat qui contient ce type de clause, il peut ensuite indiquer sur le certificat la valeur maximale des transactions pour lesquelles le certificat peut utilisé.

1) L'Algérie:

La loi 05-10 du 20 juin 2005 complétée et modifiée l'ordonnance 75-58 du 26 septembre 1975 portant code civil constitue une avancée significative en matière de preuve électronique et attendue par les juristes versée dans ces questions et les professionnels qui utilisent de plus en plus le médium électronique dans leurs relations commerciales.

L'activité des PSC n'a pas été étudié par la loi 05-10.Il faut attendre que les décrets d'application soient promulgués pour savoir comment se fera l'application de cette loi (1).En attendant, il serait souhaitable que le législateur algérien adapte les dispositions suivantes:

Fournir un effort particulier pour développer les ressources humaines dans le domaine des technologies de l'information et de la communication.

Mettre en place les structures horizontales adéquates sur le plan national pour définir la politique et les stratégies nationales favorisant le développement de la société de l'information et pour coordonner leur mise en œuvre. Afin de faciliter la coordination aux niveaux national et régional, un mécanisme d'échange d'information sera mis en place sur Internet.

---

(1) www.algéria-dz.com

Mettre en place un cadre juridique et des décrets d'application en matière du commerce électronique, car le commerce électronique ne tardera pas à voir le jour en Algérie .Il est aujourd'hui le nouveau langage universel des différentes économies du monde. L'Algérie fait toujours des progrès dans le domaine de la technologie de l'information et de la télécommunication, afin d'attraper son retard économique notamment le commerce électronique en matière de traitement et de paiement numérique. Donc l'Algérie est obligée d'adopter ce niveau de système.

Mettre en place un système de sécurité en matière du commerce électronique : la sécurité revêt une dimension majeure lorsqu'il s'agit d'échanger de l'information et de fournir des services commerciaux sur Internet .La crainte d'une brèche de sécurité est sans doute le plus grand obstacle à la pleine participation du public et des entreprises au commerce électronique sur Internet. Dans cette optique, les aspects lies à la sécurité n'étaient pas une priorité essentielle.

En effet, pour que les applications commerciales de l'Internet se développent en Algérie, la confiance doit régner.

Le législateur algérien fait des efforts pour reconnaître la valeur portant sur la signature électronique, et atteindre un niveau supérieur a travers les innovations de la technologie de l'information et de la communication, dans les domaines du commerce électronique, et du paiement numérique.

En ce qui concerne la responsabilité:le PSC fournit un certificat électronique qualifié indiquant les points suivants:

La version du certificat.

Un numéro de série.

L'algorithme utilisé.

L'identité du PSC.

La qualité du signataire.

Les données de vérifications et de création de la signature électronique.

L'identification du début et de la fin de la période de validité du certificat électronique.

Le code d'identité du certificat électronique.

La signature électronique sécurisée du PSC.

Les conditions d'utilisation du certificat électronique et le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

Les professionnels qui souhaitent exploiter des solutions de signature électronique se retrouvent donc aujourd'hui face à une incertitude en ce qui concerne la nature exacte des responsabilités qu'ils devront endosser.

Concernant tout d'abord la responsabilité contractuelle des PSC, il semble que de nombreuses difficultés puissent être réglées dans les termes du contrat entre le client et les PSC.

Il conviendra toutefois que les PSC soient particulièrement attentifs aux clauses limitatives ou élusives de responsabilité, qu'ils souhaiteraient insérer dans les contrats les liant à des non professionnels.

Il existe en effet un risque que de telles clauses soient considérées comme des clauses abusives et soient de ce fait réputées non écrites.

Sur le terrain délictuel, les PSC pourront voir la responsabilité engagée par un tiers qui s'est fié à leurs services.

La responsabilité délictuelle du PSC pourrait par exemple être engagée dans l'hypothèse où celui-ci aurait omis d'enregistrer la révocation d'un certificat en temps voulu ou aurait procédé à des vérifications insuffisantes quant à l'identité du signataire, causant ainsi un dommage au tiers qui, de bonne foi, se sera engagé sur un document invalide ou falsifié.

<u>Paragraphe 2</u> : Responsabilité des prestataires de services de certification électronique en France et USA :

1) France :

Le prestataire de services de certification est un des éléments clés de la signature électronique.

La délivrance du certificat va permettre d'identifier la personne physique ayant opposé la signature .En effet, cette délivrance est effectuée après un contrôle d'identité, plus ou moins renforcé, en fonction du type de signature envisagée (1).

Le décret du 30 Mars 2001 ne traite pas du régime de responsabilité des prestataires de services de certification électronique. C'est une de ses lacunes.

Le régime de leur responsabilité n'est abordé que dans la directive du 13 décembre 1999.

Le prestataire de services de certification est appelé à être un des acteurs essentiels de la signature électronique. A ce titre , le prestataire de service de certification , qui est avant tout un prestataire de services, est soumis au régime commun de la responsabilité civile, que celle ci soit contractuelle ou délictuelle , pour les fautes qu'il pourrait commettre à l'occasion de son activité.

1) **Responsabilité contractuelle** (le porteur du certificat)

Le prestataire de service de certification et le signataire, a qui est remis le certificat, ont préalablement conclu un contrat. Ce contrat sera généralement qualifié de contrat d'abonnement par le prestataire et va définir les conditions de délivrance du certificat. Selon le principe du non cumul des responsabilités délictuelles et contractuelles, l'article 1382 du code civil est inapplicable à la réparation du dommage se rattachant à l'exécution d'un engagement contractuel. Ainsi, un signataire victime d'un dommage ne pourra pas engager la responsabilité délictuelle du prestataire.

---

(1) Julien Esnault, op.cit., p. 42.

Seule sa responsabilité contractuelle pourra être engagée. Des lors, l'existence du droit à réparation dépend de trois conditions :

Une faute contractuelle, un dommage et un lien de causalité entre cette faute et ce dommage.

La faute consiste en une inexécution fautive d'une obligation contractuelle.

Ainsi, il faudra connaître la nature de l'obligation du prestataire, obligation de moyen ou de résultat, pour déterminer la charge de la preuve.

Pour ce faire, il faut se référer au contrat conclu entre le prestataire et le signataire.

Plus généralement, le contrat ayant pour objet la délivrance d'un certificat pourra d'analyser en un contrat d'entreprise. Ainsi, les obligations à la charge du prestataire seraient plutôt des obligations de résultat, et la preuve devrait alors, être rapportée par le signataire. La qualification en un contrat d'entreprise peut paraître favorable aux prestataires de services de certification.

En effet, le décret du 30 Mars 2001, en son article 6, II fixe de nombreuses obligations aux prestataires de certification délivrant des certificats qualifiés :

a) Faire la preuve de la fiabilité des services de certification électronique qu'il fourni.

b) Assurer le fonctionnement ; au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande.

c) Assurer le fonctionnement d'un service permettant a la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat.

Toutefois, l'aménagement contractuel peut être un moyen pour le prestataire de limiter sa responsabilité, en particulier par l'usage du certificat. En effet, les conditions d'utilisation du certificat peuvent être précisées, et limitées, dans le contrat. Dans ce cas, une information claire de signataire permettra de démontrer qu'il en avait eu connaissance.

Dès lors, il peut y avoir un partage ou une exclusion de la responsabilité du prestataire si le signataire commet une faute dans l'utilisation qu'il fera du certificat.
La négligence fautive du prestataire, peut, par exemple, permettre à un tiers de signer frauduleusement ou entraîner la création d'un certificat dont les informations seraient erronées.
La faute de l'utilisateur peut avoir pour origine une utilisation nom conforme du certificat, notamment lorsque l'usage qui en est fait dépasse les limites des transactions pour lesquelles il était prévu .En cette matière , le dommage subit doit être direct et certain. Selon l'article 1150 du code civil « le débiteur n'est tenu que des dommages et intérêts qui ont été prévus ou qu'on a pu prévoir lors du contrat, lorsque ce n'est pas par son dol que l'obligation n'est pas exécutée ».
En effet selon l'article 1148 du code civil à l'impossible nul n'est tenu » il n'y a lieu à aucune réparation lorsque, par suite d'un cas de force majeure ou d'un cas fortuit, le débiteur à été empêché de donner ou de faire ce à quoi il était obligé, ou fait ce qui lui était interdit. Donc c'est une obligation de résultat.
Cependant, dans un second temps, le prestataire négligent qui continue à utiliser un procédé technique dont les failles ont été démontrées pourrait voir sa responsabilité engagée.
La validité des clauses limitatives de responsabilité a été admise sur le fondement de l'article 1150 du code civil. Les contrats des prestataires feront donc recourt à ces clauses limitatives de responsabilité.
Il existe en effet un risque que de telles clauses soient considérées comme des clauses abusives et soient de ce fait réputées non écrites (1).

---

(1) Isabelle Renard et Isabelle Védrines ,op.cit., page.2.

Il conviendra également, dans l'hypothèse ou la fonction d'autorité de certification et d'autorité d'enregistrement serait exercée par deux entités différentes que les prestataires concernés prennent soin de définir par contrat les responsabilités qui leur incombent respectivement.

Enfin, il convient de préciser que le PSC est soumis à une exigence de protection des données personnels .Les données afférentes à la personne seront le plus généralement celles du signataire. Ainsi, le recours à un pseudonyme ne devra pas laisser transparaître l'identité réelle du signataire.

Aussi, le prestataire se doit de prendre toutes les mesures utiles pour éviter une intrusion frauduleuse dans ses bases de données.

2) **Responsabilité délictuelle** (l'utilisateur de certificat)

Sur les modèles de la responsabilité civile contractuelle, le destinataire devra démontrer l'exigence d'une faute, d'un préjudice et d'un lien de causalité entre la faute et le préjudice.

En effet, il ne pèse pas sur le prestataire d'obligation de moyen ou de résultat dans la mesure ou les parties ne sont liées par aucun contrat. Ainsi la loi du 13 Mars 2000 et le décret du 30 Mars 2001 déterminent les obligations du prestataire à l'égard du destinataire. De plus, le manquement aux obligations contractuelles, c'est à dire vis à vis de l'émette peut avoir des incidences sur le destinataire.

Ainsi la faute à l'égard de l'émetteur pourra permettre, dans certains cas , de justifier le dommage subi pas le destinataire.

La preuve de la faute sera vraisemblablement difficile à rapporter. En effet, la signature électronique met en œuvre des dispositifs informatiques complexes, c'est pourquoi , il sera la plupart du temps nécessaire de recourir a une expertise judiciaire.

De plus, le destinataire n'a pas accès au système et infrastructures du prestataires, si bien qu'il ne pourra pas directement démontrer la faute du prestataire.

Ainsi, la responsabilité délictuelle exclu toute limitation de la responsabilité par exemple d'un montant fixé au prix du certificat. Ceci serait contraire à l'ordre public, et le prestataire devra réparer entièrement le préjudice subi pas le destinataire.

Les textes sur la responsabilité des PSC ne sont pas près de voir le jour, et, dans leur rédaction actuelle, ils sont d'une portée incertaine.

Aussi la loi du 21 juin 2004 sur la confiance numérique énonce dans son article 33que:" sauf à démontrer qu'il n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants:

1) les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes.

2) les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes.

3) la délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat.

4) les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.

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

Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent , ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle".

La responsabilité des prestataires de service de certification électronique peut aussi être pénal , et la loi du 21 juin 2004 sur la confiance numérique énonce dans son article 6-1-4 que :" le fait ,pour toute personne, de présenter aux personnes mentionnés, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est punie d'une peine d'un an d'emprisonnement et de 15000 € d'amende".

2) Etats-Unis:

La loi sur les signatures numériques de l'état de l'Utah, a énoncé plusieurs exigences en matière de certificats et d'autorité de certification.

Cette loi a dégagé la responsabilité des autorités de certification en cas de réclamations du fait d'un certificat erroné ou incorrect, à condition que l'autorité de certification ait respecté les normes de la loi.

Son objectif principal était d'inciter les autorités de certification à délivrer des certificats fiables (1).

<u>Paragraphe 3</u> : La responsabilité des prestataires de service de certification dans Luxembourg et Belgique

1) Luxembourg :

La loi du 14 août 2000consacre le principe du libre exercice de l'activité de certification par toute personne physique ou morale. Elle oblige les tiers de certification à tenir un registre des certificats disponibles au public, accessible en permanence par voie électronique (2).

---

(1) Detlef Eckert et Jos Dumortier, "avant propos, éléments constitutifs de la loi européenne sur les signatures électroniques", article publié sur le site: downlood.microsoft.com 2004, p.1.

(2) www.senat.fr

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

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

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

La loi prévoit la responsabilité de tous les tiers de certification, qu'ils délivrent ou non des certificats agrées, lorsque l'utilisation d'un certificat entraîne un dommage.

L'article 21 de la loi oblige les tiers de certification au secret concernant tous les renseignements qui leur sont confiés dans le cadre de leurs activités professionnelles « le secret professionnel sera d'ordre public, et sa violation sera sanctionnée pénalement».

Ces dispositions sont inspirées de la loi modifiée du 5 Avril 1993 relative au secteur financier.

Au début e l'année 1999, la chambre de commerce Luxembourgeoise s'est engagée dans un partenariat avec la société globaisign pour délivrer des certificats numériques.

Globaisign joue le rôle d'autorité de certification « elle émet des certificats numériques reposent sur la cryptographie à clé publique, les signes à l'aide de sa clé privée et en assure la gestion».

La chambre de commerce tient les fonctions de tiers certificateur en garantissant notamment la vérification des données relatives à l'établissement du certificat numérique.

2) Belgique :

La loi du 09 juillet 2001prévoit que l'activité de certification puisse être exercée librement par une personne physique ou une personne morale. Il met en place un système facultatif d'accréditation des tires de service de certification.

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

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

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

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

<u>Paragraphe 4</u> : La responsabilité des PSC en Allemagne et Italie

1) Allemagne :

La loi allemande réglemente l'activité des tiers de certification en instaurant des licences qui sont délivrées par une autorité de contrôle.

Il s'agit de l'autorité de régulation pour les télécommunications du 25 juillet 1996, et dont les membres sont désignés par le gouvernement fédéral (1).

---

(1) www.senat.fr

La loi n'interdit pas explicitement l'activité de tiers de certification non accrédités mais cette activité se déroule alors en dehors du cadre de la loi.

Les signatures associées ne bénéficient donc pas de la garantie de fiabilité définie par la loi.

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

L'article 4 de la loi et article 1 de l'ordonnance précisent les conditions que doivent remplis les tiers de certification et les obligations qu'ils doivent respecter. Elles sont analogues aux exigences posées par l'annexe II de la directive.

En revanche, le législateur n'a pas introduit des dispositions spécifiques relative à la responsabilité des tiers de certification, faute d'être parvenu à un consensus.

La loi impose aux tiers de certification le respect de mesures de sécurité et de dispositions d'ordre technique assorties de conditions qualitative très strictes.

L'article 14 décrit les composants techniques qui doivent être utilisés, notamment pour la production et l'archivage des clés, ainsi que la production et la vérification des signatures digitales.

Des précisions sont apportées dans l'ordonnance par les articles 16 et 17. Ce dernier article fait référence à des normes techniques particulièrement précises.

Ces dispositions ont été elles-mêmes complétées par la publication, en 1998, par l'autorité de régulation pour les télécommunications et la poste, de deux catalogues de mesures techniques rédigés selon les conseils du bureau fédéral pour la sécurité dans la technique d'information. L'article 8 de l'ordonnance oblige le prestataire de service de certification à conserver les certificats qu'il a délivrés dans un registre public.

Le certificat doit figurer au registre au moins pendant la durée de qualification de l'algorithme et des paramètres pertinents qualifiés.

Avec leur durée de validité celle-ci doit être d'au moins six ans, sauf problème particulier.

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

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

Concernant le contrôle des prestataires de services : la loi allemande de 1997 avait prévu une autorisation gouvernoumentales préalable à l'exercice de cette activité (&4,1 SIG G).

Le droit allemand est aujourd'hui conforme mais il a prévu de strictes conditions a leur création. Il impose au prestataire de disposer de la fiabilité et du savoir nécessaires » et de déposer une garantie (&4, 2 ,12 SIG G).

Ceci est sanctionné par 50.000 euros d'amende (& 21.1.1 SIG G).

En outre le prestataire doit avertir l'administration au plus tard sur moment de sa prise d'activité, à défaut il est possible de 10 000 euros d'amende (& 21.2.2) (1).

Si le principe reste la liberté d'exercice, en revanche, le législateur, qu'il soit français ou allemand, a prévu un système de contrôle de l'activité des prestataires celui-ci est à deux degrés :

---

(1) Béatrice Jaluzot, op.cit., p.2871.

Ce premier degré se dédouble en deux contrôles, l'un portant sur les prestataires par une accréditation, l'autre portant sur les produits employés pour mettre en œuvre la signature électronique.

Au second degré une administration compétente est chargée de surveiller l'ensemble du système.

1) L'accréditation volontaire : les textes prévoient que les prestataires de services peuvent se faire reconnaître volontairement par un service compétent. La loi allemande prévoit à cet égard une « accréditation » (& 15.1 SIG G).

L'accréditation doit être accordée lorsque le prestataire de services prouve que les conditions posées par la loi et le décret sont remplies.

Un organisme compétent doit vérifier et attester que le dispositif sécurité est bien mis en œuvre (& 15.2).

Si nécessaire, l'accréditation peut être accordée sous condition afin que le prestataire se mette en conformité (&15.3). Elle est à renouveler à intervaller réguliers (&15.2). Les prestataires sont tenus d'une obligation de coopération afin de permettre ces vérifications. Ils doivent notamment permettre aux autorités de pénétrer dans leurs locaux, remettre tous documents nécessaires (&20.1).

L'accréditation doit être refusée lorsque les conditions légales ne sont pas remplies (&15.4). Elle peut aussi être suspendue ou retirée si les prescriptions de l'administration sont restées sans effet. Dans ce cas des mesures sont prises afin que l'actualité soit reprise par un autre organisme ou à ce que les contrats de signature soient réalisés (& 15.6).

Cette accréditation est formalisée par un sigle délivré par l'administration. Elle délivre des certificats attestant de l'accréditation et met à disposition du public les informations concernant le prestataire (&16.2).

L'administration allemande peut recourir à des organismes privés qui jouent le rôle d'organismes vérificateurs (&15.1). Ils sont reconnus en tant que tels à condition de prouver qu'ils disposent de la fiabilité, de l'indépendance et du savoir nécessaire. Cette reconnaissance peut être limitée quant à son contenu ou sa durée.

2) Le contrôle des produits de signature électronique : le droit allemand prévoit que les produits pour signature qualifiée doivent être conformes à l'état des connaissances scientifiques au moment de leur application. (&15.1SIG G).

A cet effet, l'administration peut émettre une attestation électronique garantissant leur authenticité. Le décret d'application pose les conditions techniques auxquelles ces produits doivent répondre. Les procédés doivent atteindre plusieurs objectifs.

Garantir l'utilisation des clés de signature avec des éléments biométriques, l'impossibilité d'atteindre cette clé ainsi que sa reproduction. L'annexe 1 du décret prévoit les conditions de leur vérification et fait expressément référence à des normes techniques. Les produits bénéficiant de cette attestation doivent être publiés au journal official (annexeI, 4, SIG V).

3) Le contrôle gouvernemental : l'ensemble du système allemand est placé sous contrôle gouvernemental .Ceci était déjà le cas avec la loi de 1997 et la directive européenne semble avoir avalisé ce choix en donnant implicitement la primauté à une garantie étatique du système.

La loi confie ce contrôle au ministère des postes et télécommunications. Sa mission est vaste, étant notamment chargé de l'admission des organismes vérificateurs et de l'accréditation des prestataires de services. A cette fin, il dispose d'un important pouvoir de sanction et peut prendre toute mesure enjoignant les prestataires de respecter la loi. Il peut ainsi contraindre un prestataire à cesser son activité, notamment lors qu'il est démontré qu'il ne possède pas la fiabilité nécessaire (&19,2),ou encore ordonner un blocage des certificats qualifiés lorsque la falsification a été démontrée ou ne présente pas assez de garantie. (&19.4).

Il doit mettre à disposition du public le nom des prestataires accrédités ainsi que celui de ceux qui ont été contraints de cesser leur activité (&19.6).L'administration est habilitée à percevoir des honoraires pour ces différentes démarches : pour l'accréditation volontaire des prestataires, la production de certificats qualifiés à destination des prestataires accréditée, la reconnaissance des organismes vérificateurs, en cas d'injonction aux prestataires (&22.1). Les prestataires qui ont averti l'administration de leur prise d'activité ainsi que les prestataires accrédités doivent verser une redevance annuelle afin de lui permettre de remplir leurs obligations de publicité des organismes (&22.2).

2) Italie :

Les articles 8 et 9 du décret de 1997, qui précisent respectivement les critères que doivent remplir les tiers de certification et les obligations qu'ils doivent respecter, sont similaires aux exigences posées par l'annexe II de la directive européenne. L'article 8 prévoit en particulier qu'il doit s'agir de sociétés par actions dont le capital social est au moins égal à celui exigé pour les établissements financiers (1).

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

---

(1) www.senat.fr

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

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

<u>Paragraphe 5</u>: La responsabilité des prestataires de services de certification dans la Royaume Uni, Espagne, Danemark

1) Royaume-Uni :

Le royaume uni avec"L'ELECTRONIC COMMUNICATION ACT" 2000 reprendre le même régime juridique de la responsabilité des prestataires de service de certification de la directive européenne (1).

2) Espagne :

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

Cependant les tiers de certification devront se faire inscrire sur un registre spécifique, tenu par le ministère de la justice. L'inscription ne sera réalisée qu'après la vérification de certaines conditions.

Particulièrement sévères pour les tiers qui délivreront des certificats « reconnus »,ces derniers devront en effet remplir des conditions correspondantes à celles de l'annexe II de la directive européenne .

---

(1) Voir la responsabilité des PSC dans la Directive Européenne, p.61à 69.

La loi prévoit la responsabilité de tous les tiers de certification pour les préjudices résultant du non-respect des règles relatives à l'activité de certification. C'est pourquoi les tiers de certification qui délivrent des certificats « reconnus » devront disposer de ressources suffisantes pour pouvoir faire face à leur responsabilité. A cet effet, ils devront déposer une garantie auprès d'un établissement financier. Cette garantie sera limitée à 4% du montant total des transactions susceptibles d'être réalisée grâce à leurs propres certificats.

La loi prévoit qu'un règlement pourra abaisser ce pourcentage à 22. En l'absence de plafonnement du montant des transactions pour lesquelles les certificats pourront être utilisés, la garantie devra être d'au moins un milliard de pesetas (c'est à dire environ 40 millions de francs).

Les tiers de certification auront l'obligation de garder pendant au moins quinze ans toutes les informations relatives aux certificats « reconnus ». L'activité de tous les tiers de certification sera contrôlée par le secrétariat général pour les communications, qui dépend du ministère des travaux publics.

3) Danemark :

La loi du 31 mai 2000 consacre le principe du libre exercice de l'activité de certification par toute personne, physique ou morale, et oblige tous les tiers de certification à respecter la législation relative à la protection des données personnelles.

Pour le reste, La loi ne traite que des tiers de certification qui délivreront des certificats « qualifiés » remplissent les conditions techniques, financières et humaines de sécurité et de fiabilité établies par la loi et qui correspondent à celles de l'annexe II de la directive européenne.

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

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

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

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

CONCLUSION:

Aujourd'hui, il apparaît clairement que le commerce électronique ne pourra se développer pleinement qu'avec l'utilisation de technologie de signature particulièrement, fiable, mais aussi, ne l'oublions pas, lorsque les utilisateurs d'internet pourront avoir confiance dans la valeur juridique reconnue à la signature électronique .A ce propos , les Etats européens doivent encore œuvrer vers des solutions plus harmonisées , à moins que d'ici là , les juges saisis de telles questions, ne se prononcent à leur place (1).

En ce qui concerne l'Algérie, le gouvernement algérien a lancé plusieurs opérations visant le développement des technologies de l'information et de la communication(TIC) pour, d'une part réduire la fracture numérique avec les pays développés, et, d'autre part, préparer ses citoyens à évoluer dans la société de l'information en cours de construction.Parmi ces opérations figure le projet "OUSRATIC" qui institue des facilités multiples pour permettre aux familles algériennes de se doter d'ordinateurs relié à l'Internet (2).

L'EEPAD, qui était à l'origine un établissement spécialisé dans l'enseignement professionnel à distance, participe à ce projet en tant que principal fournisseur d'Internet haut débit (ADSL). Il propose aussi dans le cadre de ce projet, des ordinateurs portables assemblés en Algérie et dotés de connexion Internet sans fil qui assure donc plus de mobilité.

---

(1) Martine Raynaud, Rev. Le MOCI. N° 1493 du 10 mai 2001"les règles relatives à la reconnaissance et aux effets juridiques évoluent", p. 70.

(2) Karim Bouaissa, "le commerce et la vague Internet, la SE en vigueur en Algérie", mémoire on-line 2007 publié sur le site:mémoire online.free.fr, p.65.

En plus de sa position de fournisseur de technologie, L'EEPAD développe une plateforme de téléenseignement dénommée CLICFORMA qui permet d'héberger des dispositifs de formation et de dispenser des formations à distance via Internet .Cette plateforme accessible à l'adresse www.clicforma.com est multi utilisateurs et multilingue arabe et français.

Cet outil d'enseignement intéresse au plus haut point les établissements scolaires du secteur de l'Education nationale ainsi que les écoles privées qui dispensent des formations en partenariat avec des écoles et universités étrangères.Ces dernière pourront ainsi réaliser des économies en matière de regroupement des stagiaires, de déplacement et d'hébergement des enseignants etc.Cette année (2007),et à titre exceptionnel ,l'accès au dispositif EcolePlus de L'EEPAD est gratuit.Prés de 500 apprenants sont déjà inscrits à la plateforme Clic forma et au dispositif de soutien scolaire EcolePlus.

Début juin 2006, L'EEPAD proposera un examen d'évaluation en ligne pour permettre aux élèves inscrits d'évaluer leurs connaissances et de se préparer à l'examen officiel du baccalauréat.

En résumé, EEPAD fournit un pack complet comprenant à la fois la fourniture de la technologie ainsi qu'un bon usage de cette technologie par les familles.

A ce jour, face à cette carence dans l'harmonisation des législations nationales, on ne peut que recommander aux entreprises désireuses de vendre dans l'espace européen de suivre très régulièrement l'évolution du droit en la matière et de s'informer sur le contenu de la législation applicable à leur contrat avant de s'engager par voie électronique.

BIBLIOGRAPHIE:

OUVRAGES:

Les ouvrages généraux:

1) En langue arabe:

-Abd El Aziz Salim: Les procédures pratiques du droit de la preuve, édition1998.
-Ben Amor Fayçal: Les clés du commerce électronique, édition Tunis, 2001.
- Kahloun Ali: Les cotés juridiques pour les chaînes de communication nouvelle et commerce électronique, édition 2001.

2) En langue française:

-Bochurberg Lionel:Internet et commerce électronique, deuxiéme édition 2001.
- Baptiste- Michelle Jean:Créer et exploiter un commerce électronique, édition litec, 1998.
- Gourion Alain - Pierre, Maria Ruano Philippeau: Le doit de l'internet dans l'entreprise, édition lgdj, 2003.
- Jacquette Jean-Michel, Philippe Delebeque: Droit du commerce international,deuxième édition 2000, dalloz.
-Louisbilon -Jean: Lamy droit de l'informatique et des réseaux informatique multimédia, éditions Lamy 2002.
- Macarez Nicolas, François Lesle: Que sais-je ? Le commerce électronique, première édition ,2001.
- Piette Thierry, Coudol, Préface Eric Blot, Lefèvre: Echanges électroniques certification et sécurité, édition litec, 1999.
-Santiago, Cavanillas Mugica, DidierGobert, Rosa Julia Barcelo, Etienne Montero, Yves Poullet, Anne Salaum, Quentin Vas Daele: Le commerce électronique temps des certitudes, édition 2000.

Les ouvrages spéciaux:

1) En langue arabe:

- El Hijazi Bayoumi Abd El Fatah: Signature électronique dans les régimes juridiques comparés, première édition, 2005.
- El Khandil Said Sahd: Signature électronique, édition 2004.

2) En langue française:

- Bensoussan Alain, Yves Le Roux: Cryptographie et signature électronique, édition hermes science publications, 1999.
- F.Fausse Arnaud-: La signature électronique, transactions et confiance sur internet, édition dunod 2001.

THESES ET MEMOIRES:

- Bouaissa Karim:Mémoire on-line 2007"le commerce et la vague Internet, la signature électronique en vigueur en Algérie.
- Esnault Julien:Mémoire de DESS de droit du multimédia et informatique "Signature électronique", en 2002-2003.
- Hafsi Samir: Mémoire de DEA en droit privé"Protection juridique du commerce électronique" en 2001-2002.

REVUES ET ARTICLES:

Revues:

Revues en langue arabe:

- Boudali Mohamed: La revue de l'école national de l'administration N°26 du 2003" La signature électronique".

Revues en langue française:

- Abella Thierry: Recueil Dalloz N°31 du 9/9/2004:" Signature électronique, quelle force pour la présomption légale?"
- Benchittrit Noël: Alternatives économiques N°193 du juin 2001:" La signature électronique arrive".
-Fares Mohamed:Revue El Mouethik N°12 du2005:" Le législateur français crée l'acte authentique électronique".
- Huet Jérôme: le Dalloz, N°6 du 2000."Vers une consécration de la preuve et de la signature électronique".
-Jaluzot- Béatrice : Transposition de la directive "Signature électronique, comparaison franco-allemande", recueil Dalloz, N°40 du 2004.
- Raynaud Martine: Le MOCI N°1493 du 10 mai 2001:" Les règles relatives à la reconnaissance et aux effets juridiques évolues".
- Le service juridique de la fédération des entreprises internationales de la mécanique et de l'électronique: Le MOCI N° 1606 du 10 juillet 2003:" A la recherche de la confiance dans l'économie numérique".

Articles:

- Azabi Sofiane, responsable du site: signelec .com:" Le nouveau régime probatoire français après l'adoption de la loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique" du 13 mars 2000, on line du 16/3/2000.
- Antoine Mireille et Didier Gober: "La directive européenne sur la signature électronique, vers la sécurisation des transactions sur l'internet ?", avril2000.
- Birnbam Laurence, Sarcy et Florence Darques:" La signature électronique"comparaison entre les législations française et américaine", avril 2001.
- Bordinat Guenièvre:" Introduction a la notion de la signature électronique", du 6 mars 2002.
-Blanchette Jean-François et banat berger François:"La dématérialisation des actes authentiques de droit français", 2002
- travaux de l'association Capitant Henri des amis de la culture juridique française: "Le contrat électronique", 2000.
- Daniel Mootti: "Signe authentique, signe numérique, et signature électronique", janvier 2002.
- Gacem .T: "La signature électronique bientôt en vigueur en Algérie, l'écrit et la signature électronique devront bientôt avoir force probante en Algérie", le 5mai2005.
- Monnier J, C:" Il faut que l'état soit le moteur du développement", le 8 mai 2005.
- Nora- C:" l'Algérie ni en retard ni en avance dans un monde numérique, la signature électronique est un sujet capital", le 23 avril2006.
-Renard Isabelle et Isabelle Védrines:" Le point sur la responsabilité des prestataires de services de certification", le 21 mai 2002.
- Vilarruba Anne Lise:" les apports de la signature électronique", le 21 octobre 2002.

LES SITES WEB:

www .Signature électronique. be
www .signelec .com
www .comment camarche.net
www.ssi.gouv.fr
Signelec. Ifrance.com
securinet.free.fr
www.senat.fr
www.awt.be
www.yohlin.net
solutions.journaldunet.com
www.itmag-dz.com

www.algérie-dz.com
www.legalliznext.com
Polaris.gseis-ucla.edu
download.microsoft.com
www.men.minefi.gouv.fr
www.consultaindtraing.com
www.unictral.org
droit-internet-2001.univ-paris 1.fr
Actualité.el-annabi.com
Achat public.com
www.epi.asso.fr
www.gouv.fr
www.clic-droit.com
actualité.el -annabi.com

ANNEXES:

La loi N°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif a la signature électronique.
La Directive Européenne N° 1999-93-CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
La loi type de la CNUDCI sur les signatures électroniques de 2001.
La loi allemande du 16 mai 2001.
La loi italienne du 15 mars 1997.
La loi fédérale américaine du 30 juin 2000.
La loi luxembourgeoise du 14 août 2000.
La loi de la Belgique du 9 juillet 2001.
La loi espagnole 59/2003.
La loi du royaume uni 2000.
La loi du Danemark 31 mai 2000.
La loi N°5-10 du 20 juin 2005, modifiée et complétée l'ordonnance N°75-58 du 26 septembre 1975 portant code civil modifiée et complétée l'article 44 de la loi N°5-10 complétée l'ordonnance 75-58 par les articles 323 bis et 323 bis 1.
Le décret N°2001-272 du 30 mars 2001, définit le cadre juridique de la mise ne place des procédés de signature électronique sécurisé
Le décret N°2002-535 du 18 avril 2002 relatif a l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
Décret N° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.
Le décret N°99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.
L'arrête du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui précédent à leur évaluation.

J.O n° 62 du 14 mars 2000 page 3968

Lois

LOI no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (1)

NOR: JUSX9900020L

L'Assemblée nationale et le Sénat ont adopté,

Le Président de la République promulgue la loi dont la teneur suit :

Article 1er

I. - L'article 1316 du code civil devient l'article 1315-1.

II. - Les paragraphes 1er, 2, 3, 4 et 5 de la section 1 du chapitre VI du titre III du livre III du code civil deviennent respectivement les paragraphes 2, 3, 4, 5 et 6.

III. - Il est inséré, avant le paragraphe 2 de la section 1 du chapitre VI du titre III du livre III du code civil, un paragraphe 1er intitulé : « Dispositions générales », comprenant les articles 1316 à 1316-2 ainsi rédigés :

« Art. 1316. - La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

« Art. 1316-1. - L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

« Art. 1316-2. - Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. »

Article 2

L'article 1317 du code civil est complété par un alinéa ainsi rédigé :

« Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. »

Article 3

Après l'article 1316-2 du code civil, il est inséré un article 1316-3 ainsi rédigé :

« Art. 1316-3. - L'écrit sur support électronique a la même force probante que l'écrit sur support papier. »

Article 4

Après l'article 1316-3 du code civil, il est inséré un article 1316-4 ainsi rédigé :

« Art. 1316-4. - La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

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

Article 5

A l'article 1326 du code civil, les mots : « de sa main » sont remplacés par les mots : « par lui-même ».

Article 6

La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans la collectivité territoriale de Mayotte.

La présente loi sera exécutée comme loi de l'Etat.

Fait à Paris, le 13 mars 2000.

Jacques Chirac

Par le Président de la République :

Le Premier ministre,

Lionel Jospin

Le garde des sceaux, ministre de la justice,

Elisabeth Guigou

Le ministre de l'intérieur,

Jean-Pierre Chevènement

Le ministre de l'économie,

Des finances et de l'industrie,

Christian Sautter

Le secrétaire d'Etat à l'outre-mer,

Jean-Jack Queyranne

Le secrétaire d'Etat à l'industrie,

Christian Pierret

(1) Loi no 2000-230.

- Directive communautaire :

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

- Travaux préparatoires :

Sénat :

Projet de loi no 488 (1998-1999) ;

Rapport de M. Charles Jolibois, au nom de la commission des lois, no 203 (1999-2000) ;

Discussion et adoption le 8 février 2000.

Assemblée nationale :

Projet de loi, adopté par le Sénat, no 2158 ;

Rapport de M. Christian Paul, au nom de la commission des lois, no 2197 ;

Discussion et adoption le 29 février 2000.

DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 décembre 1999

sur un cadre communautaire pour les signatures électroniques

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 47, paragraphe 2, et ses articles 55 et 95,

vu la proposition de la Commission (1),

vu l'avis du Comité économique et social (2),

vu l'avis du Comité des régions(3),

statuant conformément à la procédure visée à l'article 251 du traité(4),

considérant ce qui suit: atteindre cet objectif,

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Champ d'application

L'objectif de la présente directive est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Elle institue un cadre juridique pour les signatures électroniques et certains services de certification afin de garantir le bon fonctionnement du marché intérieur.

Elle ne couvre pas les aspects liés à la conclusion et à la validité des contrats ou d'autres obligations légales lorsque des exigences d'ordre formel sont prescrites par la législation nationale ou communautaire; elle ne porte pas non plus atteinte aux règles et limites régissant l'utilisation de documents qui figurent dans la législation nationale ou communautaire.

Article 2

Définitions

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 électronique 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;

3) "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;

4) "données afférentes à la création de signature", des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique;

5) "dispositif de création de signature", un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature;

6) "dispositif sécurisé de création de signature", un dispositif de création de signature qui satisfait aux exigences prévues à l'annexe III;

7) "données afférentes à la vérification de signature", des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisées pour vérifier la signature électronique;

8) "dispositif de vérification de signature", un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature;

9) "certificat", une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne;

10) "certificat qualifié", 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;

11) "prestataire de service de certification", toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques;

12) "produit de signature électronique", tout produit matériel ou logiciel, ou élément spécifique de ce produit destiné à être utilisé par un prestataire de service de certification pour la fourniture de services de signature électronique ou destiné à être utilisé pour la création ou la vérification de signatures électroniques;

13) "accréditation volontaire", toute autorisation indiquant les droits et obligations spécifiques à la fourniture de services de certification, accordée, sur demande du prestataire de service de certification concerné, par l'organisme public ou privé chargé d'élaborer ces droits et obligations et d'en contrôler le respect, lorsque le prestataire de service de certification n'est pas habilité à exercer les droits découlant de l'autorisation aussi longtemps qu'il n'a pas obtenu la décision de cet organisme.

Article 3

Accès au marché

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

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

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

4. La conformité des dispositifs sécurisés de création de signature aux conditions posées à l'annexe III est déterminée par les organismes

compétents, publics ou privés, désignés par les États membres. La Commission, suivant la procédure visée à l'article 9, énonce les critères

auxquels les États membres doivent se référer pour déterminer si un organisme peut être désigné.

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

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

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

7. Les États membres peuvent soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. Ces exigences ne doivent pas constituer un obstacle aux services transfrontaliers pour les citoyens.

Article 4

Principes du marché intérieur

1. Chaque État membre applique les dispositions nationales qu'il adopte conformément à la présente directive aux prestataires de service de certification établis sur son territoire et aux services qu'ils fournissent. Les États membres ne peuvent imposer de restriction à la fourniture de services de certification provenant d'un autre État membre dans les domaines couverts par la présente directive.

2. Les États membres veillent à ce que les produits de signature électronique qui sont conformes à la présente directive puissent circuler librement dans le marché intérieur.

Article 5

Effets juridiques des signatures électroniques

1. Les États 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

b) soient recevables comme preuves en justice.

2. Les États 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.

Article 6

Responsabilité

1. Les États membres veillent au moins à ce qu'un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat soit responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de:

a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié;

b) l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la

création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;

c) l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

LOI TYPE DE LA CNUDCI SUR LES SIGNATURES ELECTRONIQUES
2001

(Extrait du rapport de la Commission des Nations Unies sur le droit commercial international sur les travaux de sa trente-quatrième session, tenue à Vienne du 25 juin au 13 juillet 2001. Le texte de la loi type de la CNUDCI sur les signatures électroniques a été adopté le 5 juillet 2001 [Note : la version finale du guide pour l'incorporation de la loi type dans le droit interne sera publiée dans le courant du second semestre 2001])

Annexe II
Loi type de la CNUDCI sur les signatures électroniques (2001)
Article premier
Champ d'application

La présente Loi s'applique lorsque des signatures électroniques sont utilisées dans le contexte* d'activités commerciales**. Elle ne se substitue à aucune règle de droit visant à protéger le consommateur.

* La Commission propose le texte suivant aux États qui souhaiteraient étendre l'applicabilité de la présente Loi:

"La présente Loi s'applique lorsque des signatures électroniques sont utilisées, sauf dans les situations suivantes : [...]."

** Le terme "commerciales" devrait être interprété au sens large, comme désignant toute relation d'ordre commercial qu'elle soit contractuelle ou non contractuelle. Les relations d'ordre commercial comprennent, sans s'y limiter, les transactions suivantes: fourniture ou échange de marchandises ou de services; accord de distribution; représentation commerciale; affacturage;
crédit-bail; construction d'usines; services consultatifs; ingénierie; licence; investissement;
financement; opération bancaire; assurance; accord d'exploitation ou concession; coentreprise et autres formes de coopération industrielle ou commerciale; transport de marchandises ou de voyageurs par voie aérienne ou maritime, par chemin de fer ou par route.

Article 2

Définitions

Aux fins de la présente Loi:
a) Le terme "signature électronique" désigne des données sous forme

électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le

cadre du message de données et indiquer qu'il approuve l'information qui y est contenue;
b) Le terme "certificat" désigne un message de données ou un autre enregistrement confirmant le lien entre un signataire et des données afférentes à la création de signature;
ii) Il estime, au regard des circonstances connues de lui, qu'il y a un risque important que les données afférentes à la création de signature aient été compromises;
c) Prend, lorsqu'un certificat est utilisé pour étayer la signature électronique, des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes.

2. Un signataire assume les conséquences juridiques de tout manquement aux exigences visées au paragraphe 1.

Article 9
Normes de conduite du prestataire de services de certification
1. Lorsqu'un prestataire de services de certification fournit des services visant à étayer une signature électronique qui peut être utilisée pour produire des effets juridiques en tant que signature, ce prestataire :

a) Agit en conformité avec les déclarations qu'il fait concernant ses politiques et pratiques ;
b) Prend des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou figurant dans le certificat sont exactes et complètes;
c) Fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles de déterminer à partir de ce certificat :
i) L'identité du prestataire de services de certification;
ii) Si le signataire identifié dans le certificat avait, au moment de l'émission de ce dernier, le contrôle des données afférentes à la création de signature;
iii) Les données afférentes à la création de signature étaient valides au moment ou avant le moment de l'émission du certificat;
d) Fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles de déterminer, s'il y a lieu, à partir de ce certificat ou de toute autre manière :
i) La méthode utilisée pour identifier le signataire;
ii) Toute restriction quant aux fins ou à la valeur pour lesquelles les données afférentes à la création de signature ou le certificat peuvent être utilisés;
iii) Si les données afférentes à la création de signature sont valides et n'ont pas été compromises;

iv) Toute restriction quant à l'étendue de la responsabilité stipulée par le prestataire de services de certification;
v) S'il existe des moyens pour le signataire d'adresser une notification conformément à l'alinéa b) du paragraphe 1 de l'article 8 de la présente Loi;
vi) La disponibilité d'un service de révocation en temps utile;

Art. 44. — L'ordonnance n° 75-58 du 26 septembre 1975 susvisée, est complétée par les *articles 323 bis et 323 ter,* rédigés comme suit :
"Art. 323 bis. — La preuve par écrit résulte d'une suite de lettres ou de caractères ou de chiffres ou de tout autre signe ou symbole doté d'une signification intelligible, quels que soient leurs supports et leurs modalités de transmission".
"Art. 323 ter. — L'écrit sous forme électronique est admis en tant que preuve au même titre que l'écrit sur support papier, à la condition 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".

Publication au JORF du 31 mars 2001

Décret n°2001-272 du 30 mars 2001

Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

NOR:JUSC0120141D

version consolidée au 4 mai 2007 - *version JO initiale*

Le Premier ministre,

Sur le rapport de la garde des sceaux, ministre de la justice,

Vu la directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ;

Vu le code civil, notamment ses articles 1316 à 1316-4 ;

Vu la loi n° 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Article 1

Au sens du présent décret, on entend par :

1. Signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ;

2. Signature électronique sécurisée : une signature électronique qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;

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

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

3. Signataire : toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en oeuvre un dispositif de création de signature électronique ;

4. Données de création de signature électronique : les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;

5. Dispositif de création de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;

6. Dispositif sécurisé de création de signature électronique : un dispositif de création de signature électronique qui satisfait aux exigences définies au I de l'article 3 ;

7. Données de vérification de signature électronique : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;

8. Dispositif de vérification de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique ;

9. Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;

10. Certificat électronique qualifié : un certificat électronique répondant aux exigences définies à l'article 6 ;

11. Prestataire de services de certification électronique : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;

12. Qualification des prestataires de services de certification électronique : l'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité.

Article 2

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

Publication au JORF du 19 avril 2002

Décret n°2002-535 du 18 avril 2002

Décret relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information

NOR:PRMX0100183D

version consolidée au 19 avril 2002 - *version JO initiale*

Le Président de la République,

Sur le rapport du Premier ministre, du ministre de l'économie, des finances et de l'industrie et du ministre délégué à l'industrie, aux petites et moyennes entreprises, au commerce, à l'artisanat et à la consommation,

Vu la directive 98/34/CE du 22 juin 1998, modifiée par la directive 98/48/CE du 20 juillet 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la consommation, notamment son article R. 115-6 ;

Vu le décret n° 97-34 du 15 janvier 1997, modifié par le décret n° 97-463 du 9 mai 1997 et par le décret n° 97-1205 du 19 décembre 1997, relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 97-1184 du 19 décembre 1997, modifié par le décret n° 2001-143 du 15 février 2001, pris pour l'application au Premier ministre du 1° de l'article 2 du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Le Conseil d'Etat (section de l'intérieur) entendu ;

Le conseil des ministres entendu,

Article 1

La sécurité offerte par des produits ou des systèmes des technologies de l'information, au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance peut être certifiée dans les conditions prévues au présent décret.

Les administrations de l'Etat recourent, dans la mesure du possible et en fonction de leurs besoins de sécurité, à des produits ou des systèmes des technologies de l'information certifiés suivant la procédure prévue au présent décret.

TABLE DES MATIERES: