COMMISSION DES COMMUNAUTES EUROPÉENNES

Bruxelles, le 13.05.1998
COM(1998) 297 final

98/0191 (COD)

Proposition de

DIRECTIVE DU PARLEMENT EUROPEEN ET DU CONSEIL

sur un cadre commun pour les signatures électroniques

(présentée par la Commission)

EXPOSÉ DES MOTIFS

I. CONTEXTE

Les réseaux ouverts comme Internet sont de plus en plus importants pour la communication dans le monde. Ils permettent une communication interactive entre des personnes qui parfois n'entretenaient préalablement aucune relation. En fournissant des outils pour accroître la productivité et réduire les coûts, ainsi que de nouveaux moyens d'atteindre les clients, ils offrent de nouvelles possibilités économiques. Les réseaux sont mis à profit par les entreprises qui souhaitent exploiter de nouvelles façons de faire des affaires et de nouvelles méthodes de travail: télétravail, environnements virtuels partagés, etc. Les organismes d'État recourent également à ces réseaux dans leurs relations avec les entreprises et les particuliers. Le commerce électronique offre à l'Union européenne une excellente occasion de poursuivre son intégration économique.

Pour tirer le meilleur parti de ces possibilités, il est nécessaire d'instaurer un environnement sûr en ce qui concerne l'authentification électronique. Il existe différentes de signer un document électroniquement, qui varient de méthodes très simples (par exemple l'insertion d'une image scannée d'une signature faite à la main dans un document réalisé par traitement de texte), à des méthodes très avancées (par exemple les signatures numériques à "clé cryptographique publique"). Les signatures électroniques permettent au destinataire de données transmises électroniquement de vérifier l'origine des données (*authentification de l'origine des données*) et de vérifier que les données sont complètes et inchangées, et préserver ainsi leur intégrité *(intégrité des données)*.

La vérification de l'authenticité et de l'intégrité des données ne prouve pas nécessairement l'identité du signataire qui a généré les signatures électroniques. Comment le destinataire peut-il, par exemple, savoir si l'expéditeur est réellement la personne qu'il prétend être ? Le destinataire peut donc souhaiter obtenir des informations plus sûres concernant l'identité du signataire. Cette information peut être fournie par le signataire en personne, en fournissant au destinataire une preuve satisfaisante. Un autre moyen consiste à recevoir confirmation par une tierce partie (par exemple une personne ou une institution ayant la confiance mutuelle des deux parties). Dans le cadre de la présente directive, ces tierces parties sont appelées "*prestataires de services de certification*".

Dans sa communication du 16 avril intitulée "Une initiative européenne dans le domaine du commerce électronique"[1] et adressée au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, la Commission reconnaissait que les signatures numériques constituaient un moyen essentiel d'assurer la sécurité et de développer la confiance sur les réseaux ouverts. Dans la déclaration ministérielle de Bonn[2], les signatures numériques apparaissaient également comme une question prioritaire pour le commerce électronique.

---

1 COM(97) 157 final du 16.4.1997.

2 Conférence ministérielle européenne "Global information networks: realising the potential", Bonn 6-8.7.1997.

Dans un premier temps, la Commission a présenté au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions une communication intitulée "Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et le chiffrement"[3] dans laquelle elle soulignait la nécessité d'une approche cohérente dans ce domaine. Le 1er décembre 1997, le Conseil a accueilli favorablement cette communication et invité la Commission à soumettre dès que possible une proposition de directive du Parlement européen et du Conseil sur les signatures numériques.

À la suite de la publication de la communication et de réunions organisées avec les États membres, des représentants du secteur privé, notamment de l'industrie européenne de la cryptographie, et de l'audition internationale d'experts de Copenhague[4], la Commission a reçu des contributions des différentes parties concernées. Les conclusions suivantes ont pu être tirées des informations recueillies:

1. Dans ce domaine, les initiatives législatives se multiplient dans plusieurs États membres et il devient donc urgent d'avoir un cadre juridique harmonisé au niveau européen afin d'éviter ainsi que le fonctionnement du marché intérieur ne soit gravement entravé.

2. Bien que les techniques de signature numérique utilisant la cryptographie à clé publique soient au centre des discussions et fassent l'objet de nombreuses activités, une directive européenne doit être neutre du point de vue technique et ne pas se limiter à ce type de signatures. Comme il est souhaitable qu'une diversité de mécanismes d'authentification fassent leur apparition, le champ d'application de la présente directive doit être suffisamment large pour couvrir une gamme de "signatures électroniques" qui englobent les signatures numériques basées sur la cryptographie à clé publique ainsi que d'autres moyens d'authentification des données.

3. Afin d'assurer le bon fonctionnement du marché intérieur et de soutenir le développement rapide du secteur d'activité en termes de demande et d'innovation technologique, tout régime d'autorisation préalable doit être évité. Pour gagner la confiance des consommateurs, il pourrait être utile d'avoir des régimes volontaires d'accréditation pour les prestataires de service de certification dans le but de fournir un niveau de sécurité plus élevé. Dans la mesure ou cette démarche correspond à ce qu'exige le marché, cela pourrait constituer une indication plus précise ou plus prévisible du niveau de sécurité juridique pour le prestataire de service de certification et le consommateur.

4. Les signatures électroniques utilisées, par exemple, à l'intérieur de groupes fermés, où des relations contractuelles sont déjà établies, ne doivent pas forcément entrer dans le champ d'application de la présente directive. Dans un tel contexte, c'est la liberté contractuelle qui doit prévaloir.

---

3 COM(97) 503 final du 8.10.1997.

4 Conférence internationale de Copenhague, 23-24.4.1998.

5. À cet égard, on considère que le plus important est d'assurer la reconnaissance juridique, au niveau international en particulier, des signatures électroniques et des services de certification. Cela implique de préciser les exigences essentielles pour les prestataires de services de certification, y compris leur responsabilité.

6. Les entreprises doivent prendre l'initiative, avec les organismes de normalisation, d'élaborer des normes internationalement reconnues pour les signatures numériques. Ces normes doivent viser à instaurer un environnement ouvert à des produits et services interopérables. Le rôle de la Commission sera de soutenir ce processus.

7. Au niveau international, de nombreuses activités et discussions sont en cours. La commission des Nations unies pour le droit commercial international (CNUDCI) a adopté une loi-type sur le commerce électronique et a entamé des travaux visant à préparer des règles uniformes pour les signatures numériques. L'Organisation de coopération et développement économiques (OCDE) travaille également sur ce sujet, dans le prolongement de ses Orientations pour une politique en matière de cryptographie de 1997. D'autres organisations internationales, dont l'Organisation mondiale du commerce (OMC), commencent aussi à s'intéresser à des questions connexes. Cette évolution récente doit être prise en compte dans la mise en œuvre d'un cadre juridique au niveau européen.

II. BESOIN D'HARMONISATION

Plusieurs États membres ont déjà pris des initiatives législatives détaillées en ce qui concerne les signatures électroniques:

État membre	État d'avancement du processus législatif
Allemagne	• Loi et décret sur les signatures numériques adoptés: conditions dans lesquelles les signatures numériques sont jugées sûres; accréditation volontaire des prestataires de services; • Établissement du catalogue des mesures de sécurité adaptées; • Consultation publique en cours sur les aspects juridiques des signatures numériques et des documents électroniques signés numériquement.
Autriche	Travaux préparatoires.
Belgique	• Loi sur les télécommunications: régime volontaire de déclaration préalable pour les prestataires de services; • Projet de loi sur les services de certification relatifs aux signatures numériques; • Projet de loi modifiant le Code civil en ce qui concerne les preuves électroniques. • Elaboration d'une loi sur l'usage des signatures numériques pour la sécurité sociale et la santé publique.
Danemark	Projet de loi sur l'utilisation sûre et efficace des communications numériques.

Espagne	• Circulaires de la direction des Douanes sur l'utilisation des signatures électroniques; • Résolution dans le domaine de la sécurité sociale régissant l'utilisation des moyens électroniques; • Lois et circulaires dans le domaine des hypothèques, de la fiscalité, des services financiers et de l'enregistrement des entreprises autorisant l'utilisation de procédures électroniques; • Loi de finances de 1998 mandatant le ministère de l'Intérieur à agir comme prestataire de service de certification.
Finlande	• Projet de loi sur l'échange électronique d'informations dans l'administration et les procédures judiciaires administratives; • Projet de loi sur le statut du centre de recensement de la population en tant que prestataire de service de certification.
France	• Loi sur les télécommunications (décrets sur les autorisations et exemptions): ⇒ fourniture de produits de signature électronique soumise à une procédure d'information; ⇒ liberté d'utilisation, d'importation et d'exportation des produits et services de signature électronique. • Législation concernant l'utilisation des signatures numériques pour la sécurité sociale et la santé publique.
Italie	• Loi générale sur la réforme du service public et la simplification administrative adoptée: principe de la reconnaissance juridique des documents électroniques; • Décret sur la création, l'archivage et la transmission des documents et contrats électroniques; • Décret en préparation sur les exigences relatives aux produits et services; • Décret en préparation sur les obligations fiscales découlant des documents électroniques.
Pays-Bas	• Régime volontaire d'accréditation en préparation pour les prestataires de services; • Loi sur la fiscalité prévoyant la soumission des déclarations de revenus par voie électronique; • Projet de loi modifiant le Code civil en préparation.
Royaume-Uni	Préparation d'une loi concernant l'accréditation volontaire des prestataires de services de certification et la reconnaissance juridique des signatures numériques.
Suède	Travaux préparatoires.

Cet aperçu montre que les différentes initiatives en cours dans les États membres conduisent à une situation juridique très hétérogène. Bien que les États membres semblent se concentrer sur les mêmes questions, notamment les exigences imposées aux prestataires de services et aux produits, les critères qui détermineront l'effet juridique des signatures électroniques, et la structure des régimes d'accréditation, il est évident que la diversité des réglementations respectives - ou leur inexistence - sera telle que le fonctionnement du marché intérieur dans le domaine des signatures électroniques s'en trouvera menacé. Toute divergence dans les règles définissant l'effet juridique attribué aux signatures

numériques est particulièrement préjudiciable au développement futur du commerce électronique et, partant, à la croissance économique et à l'emploi dans la Communauté. Des incertitudes peuvent également résulter de régimes différents en matière de responsabilité ainsi que du risque d'incohérences dans la jurisprudence en matière de responsabilité. De plus, il est probable que les critères techniques en fonction desquels les signatures électroniques seront considérées comme sûres varieront d'un État membre à l'autre.

L'hétérogénéité de la situation, en entravant l'utilisation et la fourniture de services liés aux signatures électroniques et en freinant le développement de nouvelles activités économiques en rapport avec le commerce électronique, risque de constituer un sérieux obstacle à la communication et aux affaires par réseaux ouverts dans l'Union européenne. L'objectif de la proposition de directive ci-jointe est de lever les obstacles, en particulier les différences concernant la reconnaissance juridique des signatures électroniques, ainsi que les restrictions à la libre circulation des services et produits de certification entre les Etats membres. Compte tenu des objectifs poursuivis, la mesure prévue relève de la compétence exclusive de la Communauté. La proposition de directive vise a "permettre" l'usage des signatures électroniques dans un espace sans frontières en se concentrant sur les obligations essentielles pour les services de certification, et laisse les détails de la mise en oeuvre à la discrétion des Etats membres. Ceci est en phase avec la politique juridique de la Commission en matière de subsidiarité, de proportionalité et de simplification législative.

Par conséquent, la Commission propose que la présente proposition prenne pour base juridique l'article 57 paragraphe 2 et les articles 66 et 100 A du traité. Pour des raisons de proportionnalité, la Commission estime qu'une directive est l'instrument juridique le plus approprié.

III. OBJECTIF ET CHAMP D'APPLICATION DE LA DIRECTIVE

1. La présente directive vise à assurer le bon fonctionnement du marché intérieur dans le domaine des signatures électroniques, en instituant un cadre juridique homogène et approprié à l'utilisation de ces signatures dans la Communauté européenne et en définissant un ensemble de critères qui constituent la base de leur reconnaissance juridique.

2. Les communications et le commerce électroniques mondiaux dépendent de l'adaptation progressive des législations nationales et internationales à l'évolution rapide de l'infrastructure technique. Même si, dans de nombreux cas, procéder par analogie avec les règles existantes peut fournir une solution satisfaisante, il sera peut-être nécessaire d'adapter ces législations en fonction des nouvelles technologies afin d'éviter les effets contraires ou indésirables. Bien que les signatures numériques produites à l'aide de techniques cryptographiques soient aujourd'hui considérées comme un type de signature électronique de première importance, le cadre réglementaire européen doit être suffisamment souple pour prendre en compte d'autres techniques susceptibles d'être utilisées pour assurer l'authentification.

3. La technologie des signatures électroniques a des applications évidentes dans les environnements fermés, comme un réseau local d'entreprise ou un système bancaire. Les certificats et les signatures électroniques ont également une fonction

d'autorisation, par exemple pour accéder à un compte privé. Dans le cadre des législations nationales, le principe de la liberté contractuelle permet aux parties contractantes de convenir entre elles des modalités de leurs transactions, c'est-à-dire si elles acceptent ou non les signatures électroniques. Dans ce cas, il n'y a manifestement pas besoin de réglementation.

4. Compte tenu de la gamme de services en question et de leurs possibles applications, les prestataires de service de certification doivent pouvoir offrir leurs services sans être obligés d'obtenir une autorisation préalable. Toutefois, les prestataires de services souhaiteront peut-être bénéficier de la validité juridique que confèrent aux signatures électroniques des régimes volontaires d'accréditation liés à des exigences communes. L'accréditation doit être considérée comme un service public offert aux prestataires de service de certification désireux de fournir des services de haut niveau. Ceci ne doit en aucun cas impliquer qu'un prestataire de service non accrédité est automatiquement moins sûre.

5. Un prestataire de service de certification peut offrir une large gamme de services. La présente directive porte plus particulièrement sur les services de certification en relation avec les signatures électroniques. Les certificats peuvent être utilisés à des fins très diverses et contenir différents éléments d'information. Il peut s'agir d'identificateurs classiques, comme le nom, l'adresse, le numéro d'enregistrement ou le numéro de sécurité sociale, le numéro de TVA ou d'identification fiscale, ou d'attributs spécifiques au signataire permettant de savoir, par exemple, s'il est mandaté pour agir au nom d'une entreprise, s'il est solvable, s'il a des garants ou s'il est titulaire de permis ou de licences particuliers. Par conséquent, divers certificats sont envisageables pour toute une série d'utilisations. Néanmoins, un cadre juridique est surtout nécessaire pour les certificats, afin de permettre l'authentification de la signature électronique de la personne qui signe. La présente directive a donc pour objet la fonction d'un certificat (appelé "certificat agréé") en relation avec l'identité civile ou le rôle d'une personne donnée.

6. Dans un système ouvert, mais fiable, de signatures électroniques, l'effet juridique attesté par une signature est un élément essentiel. L'application de la présente directive contribuera également à instituer un cadre juridique harmonisé dans la Communauté en garantissant que la force exécutoire, l'effet ou la validité juridique d'une signature électronique ne soit pas contestée au seul motif que la signature se présente sous la forme de données électroniques, qu'elle ne repose pas sur un certificat agréé ou sur un certificat délivré par un prestataire de service de certification accrédité, et que les signatures électroniques soient reconnues au niveau juridique de la même façon que les signatures manuscrites. En outre, les régimes nationaux d'admissibilité des preuves doivent être élargis pour prendre en compte l'utilisation des signatures électroniques.

7. La reconnaissance juridique des signatures électroniques doit reposer sur des critères objectifs, transparents, non discriminatoires et proportionnels et n'être conditionnée à aucune autorisation ou accréditation du prestataire de service concerné. Les exigences communes applicables aux prestataires de service de certification doivent permettre la reconnaissance internationale des signatures et certificats dans la Communauté européenne. Les exigences doivent s'appliquer aux prestataires de service de certification indépendamment du type d'accréditation en vigueur dans tel ou tel État membre. Les progrès techniques ou l'évolution du

marché pouvant exiger certaines adaptations, il sera peut-être nécessaire de réviser ces exigences de temps en temps. La Commission pourra proposer de nouvelles exigences sur la base des recommandations qui lui seront faites.

8. En matière de responsabilité, des règles communes doivent contribuer à susciter la confiance des consommateurs et des entreprises, qui accordent crédit aux certificats, et des prestataires de services, et promouvoir ainsi une large diffusion des signatures électroniques.

9. Des mécanismes coopératifs permettant la reconnaissance d'État à État des signatures et certificats avec les pays tiers sont essentiels au développement du commerce électronique international. En particulier, permettre aux prestataires de service de certification à l'intérieur de la Communauté européenne d'avaliser les certificats de pays tiers de la même façon qu'ils garantissent leurs propres certificats pourrait constituer un moyen simple mais efficace de promouvoir les services internationaux.

Proposition de

DIRECTIVE DU PARLEMENT EUROPEEN ET DU CONSEIL

sur un cadre commun pour les signatures électroniques

(Texte présentant de l'intérêt pour l'EEE)

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

vu le traité instituant la Communauté européenne et notamment ses articles 57 paragraphe 2, 66 et 100 A,

vu la proposition de la Commission[5],

vu l'avis du Comité économique et social[6],

vu l'avis du Comité des régions[7],

statuant conformément à la procédure visée à l'article 189 B du traité[8],

(1) considérant que, le 16 avril 1997, la Commission a présenté au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, une communication sur une initiative européenne dans le domaine du commerce électronique[9];

(2) considérant que, le 8 octobre 1997, la Commission a présenté au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, une communication intitulée "Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et le chiffrement"[10];

(3) considérant que, le 1er décembre 1997, le Conseil a invité la Commission à soumettre dès que possible une proposition de directive du Parlement européen et du Conseil sur les signatures numériques;

(4) considérant que les communications et le commerce électroniques nécessitent des signatures électroniques et des services connexes permettant d'authentifier les données; que toute divergence dans les règles relatives à la reconnaissance juridique des signatures électroniques et à l'accréditation des "prestataires de service de certification" dans les États membres risque de constituer un sérieux

---

5 JO C
6 JO C
7 JO C
8 JO C
9 COM(97) 157 final
10 COM(97) 503 final

obstacle à l'utilisation des communications électroniques et au commerce électronique, et donc d'entraver le développement du marché intérieur; que la diversité des activités menées dans les États membres met en évidence le besoin d'harmonisation au niveau communautaire;

(5) considérant qu'il faut promouvoir l'interopérabilité des produits de signature électronique; que, conformément à l'article 7 A du traité, le marché intérieur comporte un espace dans lequel la libre circulation des marchandises doit être assurée; que des exigences essentielles spécifiques aux produits de signature électronique utilisés par les prestataires de service de certification doivent être respectées afin d'assurer la libre circulation dans le marché intérieur et de susciter la confiance dans les signatures électroniques;

(6) considérant que, eu égard à la rapidité des progrès techniques et à la dimension mondiale d'Internet, il convient d'adopter une approche qui prenne en compte les diverses technologies et services permettant d'authentifier des données électroniquement; que, toutefois, les "signatures numériques" reposant sur la cryptographie à clé publique constituent actuellement la forme la plus reconnue de signature électronique;

(7) considérant que le marché intérieur permet aux prestataires de service de certification de développer leurs activités transfrontalières afin d'accroître leur compétitivité, et d'offrir ainsi aux particuliers et aux entreprises de nouvelles possibilités d'échanger des informations et de commercer électroniquement en toute sécurité indépendamment des frontières; que les prestataires de service de certification doivent généralement être libres d'offrir leurs services sans autorisation préalable afin de favoriser la fourniture à l'échelle communautaire de services de certification sur des réseaux ouverts; que, dans l'immédiat, il n'est pas nécessaire d'assurer la libre circulation des services de certification en harmonisant les restrictions nationales à la fourniture de ces services qui s'avèrent justifiées et proportionnées;

(8) considérant que les régimes volontaires d'accréditation visant à élever le niveau du service fourni peuvent offrir aux prestataires de service de certification le cadre approprié au perfectionnement de leurs services en fonction du niveau de confiance, de sécurité et de qualité imposé par l'évolution du marché; que de tels régimes doivent inciter à mettre au point des règles de bonne conduite entre prestataires de service de certification; que les prestataires de service de certification doivent rester libres d'adhérer à ces régimes d'accréditation et d'en bénéficier; que les États membres ne doivent pas interdire aux prestataires de service de certification d'opérer en dehors de ces régimes d'accréditation; qu'il faut veiller à ce que les régimes d'accréditation ne limitent pas la concurrence dans le secteur des services de certification; qu'il est important de trouver un équilibre entre les besoins des particuliers et ceux des entreprises;

(9) considérant que la présente directive doit donc promouvoir l'utilisation et la reconnaissance juridique des signatures électroniques dans la Communauté; qu'un cadre réglementaire n'est pas nécessaire pour les signatures électroniques utilisées exclusivement à l'intérieur de systèmes fermés; que la liberté des parties de convenir entre elles des conditions dans lesquelles elles acceptent les données signées électroniquement doit être sauvegardée dans les limites autorisées par la

législation nationale; que la présente directive ne vise pas à harmoniser les règles nationales concernant le droit des contrats, en particulier l'établissement et l'exécution des contrats, ou d'autres formalités non contractuelles nécessitant signature; que, pour cette raison, les dispositions concernant les effets juridiques des signatures électroniques ne doivent préjuger ni des obligations de forme requises par le droit national pour la conclusion des contrats, ni des règles déterminant le lieu où un contrat est conclu;

(10) considérant que, afin de contribuer à l'acceptation générale des signatures électroniques, une signature électronique ne doit pas être considérée comme dépourvue de validité juridique au seul motif que la signature se présente sous la forme de données électroniques, qu'elle ne repose pas sur un certificat agréé ou sur un certificat délivré par un prestataire de service de certification accrédité, ou que le prestataire de service qui a délivré le certificat en question est originaire d'un autre État membre; que les signatures électroniques, liées à un prestataire de service de certification fiable qui satisfait aux exigences essentielles, doivent avoir le même effet juridique que les signatures manuscrites; qu'il faut veiller à ce que les signatures électroniques puissent avoir force de preuve en justice dans tous les États membres; que la reconnaissance juridique des signatures électroniques doit reposer sur des critères objectifs et ne pas être subordonnée à l'autorisation du prestataire de service concerné; que des règles harmonisées sur l'effet juridique des signatures électroniques seront la garantie d'un cadre juridique cohérent dans la Communauté;

(11) considérant que les prestataires de service de certification offrant des services de certification au public sont soumis à la législation nationale en matière de responsabilité; que des différences dans le champ d'application et le contenu de ces réglementations risquent de susciter des incertitudes juridiques, notamment en ce qui concerne les tiers utilisant les services de ces prestataires; que de telles incertitudes seront préjudiciables au développement du commerce transfrontalier et entraveront le bon fonctionnement du marché intérieur; que l'harmonisation des règles en matière de responsabilité offre sécurité et prévisibilité juridiques aux prestataires de service de certification et aux consommateurs; que de telles règles doivent contribuer à l'acceptation générale et à la reconnaissance juridique des signatures électroniques dans la Communauté et, par conséquent, avoir un effet bénéfique sur le fonctionnement du marché intérieur;

(12) considérant que des mécanismes transfrontaliers impliquant des pays tiers sont indispensables au développement du commerce électronique international; que ces mécanismes doivent être mis au point au niveau des entreprises; que des accords multilatéraux avec des pays tiers sur la reconnaissance mutuelle des services de certification pourraient contribuer à assurer l'interopérabilité au niveau mondial;

(13) considérant que, pour favoriser les communications et le commerce électroniques en assurant la confiance des utilisateurs, les États membres doivent obliger les prestataires de service de certification à respecter la législation sur la protection des données et le respect de la vie privée, et être en mesure de fournir également des services de certification pour les pseudonymes à la demande du signataire; que la loi nationale devrait préciser si, et à quelles conditions, les données révélant l'identité de la personne faisant l'objet des données doivent être transmises pour des enquêtes pénales; que les prestataires de service de certification doivent

préalablement informer les utilisateurs de leurs conditions, notamment en ce qui concerne l'utilisation précise de leurs certificats et les limites de leur responsabilité, et ce par écrit, dans une langue aisément compréhensible et par un moyen de communication durable;

(14) considérant que, aux fins de l'application de la présente directive, la Commission doit être assistée d'une comité de caractère consultatif;

(15) considérant que, conformément aux principes de subsidiarité et de proportionnalité visés à l'article 3 B du traité, l'objectif consistant à instituer un cadre juridique harmonisé pour la fourniture de signatures électroniques et de services connexes ne peut pas être réalisé de manière suffisante par les États membres et peut être mieux réalisé au niveau communautaire; que la présente directive se limite aux exigences minimales nécessaires pour atteindre cet objectif,

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE:

Article premier
Champ d'application et objectif

La présente directive porte sur l'utilisation et la reconnaissance juridique des signatures électroniques.

Elle ne couvre pas d'autres aspects liés à la conclusion et à la validité des contrats ou d'autres formalités non contractuelles nécessitant signature.

Elle institue un cadre juridique pour certains services de certification accessibles au public.

Article 2
Définitions

Aux fins de la présente directive, on entend par:

1) "signature électronique", une signature sous forme numérique intégrée, jointe ou liée logiquement à des données, utilisée par un signataire pour signifier son acceptation du contenu des données, et 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 détectée;

2) "signataire", toute personne qui crée une signature électronique;

3) "dispositif de création de signature", des données uniques, telles que des codes ou des clés cryptographiques privées, ou un dispositif matériel configuré spécifiquement, que le signataire utilise pour créer une signature électronique;

4) "dispositif de vérification de signature", des données uniques, telles que des codes ou des clés cryptographiques publiques, ou un dispositif matériel configuré spécifiquement, qui est utilisé pour vérifier la signature électronique;

5) "certificat agréé", une attestation numérique qui lie un dispositif de vérification de signature à une personne, confirme l'identité de cette personne et satisfait aux exigences prévues à l'annexe I;

6) "prestataire de service de certification", toute personne ou entité qui délivre des certificats au public ou lui fournit d'autres services liés aux signatures électroniques;

7) "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.

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 élever 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 de service de certification pour des motifs relevant du champ d'application de la présente directive.

3. Conformément à la procédure prévue 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 le considèrent comme conforme aux exigences visées au point (e) de l'annexe II.

4. Les États membres peuvent admettre l'usage des signatures électroniques dans le secteur public sous réserve d'exigences supplémentaires. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires, et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée.

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 conformes à la présente directive puissent circuler librement sur le marché intérieur.

Article 5
Effets juridiques

1. Les États membres veillent à ce qu'une signature électronique ne soit pas considérée comme dépourvue d'effet ou de validité juridique, ou de force exécutoire, au seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat agréé, ou qu'elle ne repose pas sur un certificat délivré par un prestataire de service de certification accrédité.

2. Les États membres veillent à ce que les signatures électroniques reposant sur un certificat agréé délivré par un prestataire de service de certification qui satisfait aux exigences prévues à l'annexe II soient, d'une part, reconnues comme conformes aux exigences légales relatives à une signature manuscrite et, d'autre part, admises comme preuve en justice de la même façon que les signatures manuscrites.

Article 6
Responsabilité

1. Les États membres veillent à ce qu'un prestataire de service de certification qui délivre un certificat agréé soit responsable envers toute personne qui, de bonne foi, accorde crédit au certificat en ce qui concerne:

   a) l'exactitude des informations contenues dans le certificat agréé à compter de la date où il a été délivré, sauf indication contraire du prestataire de service de certification mentionnée dans le certificat;

   b) la conformité à toutes les exigences de la présente directive pour ce qui est de la délivrance du certificat agréé;

   c) l'assurance que la personne identifiée dans le certificat agréé détenait, au moment de la délivrance du certificat, le dispositif de création de signature correspondant au dispositif de vérification de signature mentionné ou identifié dans le certificat;

   d) au cas où le prestataire de service de certification génère le dispositif de création de signature et le dispositif de vérification de signature, l'assurance que les deux dispositifs fonctionnent ensemble de façon complémentaire.

2. Les États membres veillent à ce qu'un prestataire de service de certification ne soit pas tenu pour responsable des erreurs concernant les informations contenues dans le certificat qualifié qui ont été fournies par la personne à qui le certificat a été délivré, s'il peut démontrer qu'il a vérifié ces informations avec toute la diligence requise.

3. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat agréé particulier, les limites fixées à son utilisation. Le prestataire de service de certification ne doit pas être tenu pour responsable des dommages résultant de l'usage d'un certificat agréé en dehors des limites fixées à son utilisation.

4. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat agréé, la valeur limite des transactions pour lesquelles le certificat est valable. Le prestataire de service de certification ne doit pas être tenu pour responsable des dommages résultant du dépassement de cette valeur limite.

5. Les dispositions des paragraphes 1 à 4 s'appliquent sans préjudice de la directive 93/13/CEE du Conseil[11].

Article 7
Aspects internationaux

1. Les États membres veillent à ce que les certificats délivrés par un prestataire de service de certification établi dans un pays tiers soient reconnus comme juridiquement équivalents aux certificats délivrés par un prestataire de service de certification établi dans la Communauté:

   a) si le prestataire de service de certification remplit les conditions prévues dans la présente directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi par un État membre; ou

   b) si un prestataire de service de certification établi dans la Communauté, qui satisfait aux exigences visées à l'annexe II, garantit les certificats de pays tiers de la même façon qu'il garantit ses propres certificats; ou

   c) si le certificat ou le prestataire de service de certification est reconnu dans le cadre d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.

2. Afin de promouvoir les services de certification transfrontaliers impliquant des pays tiers et la reconnaissance juridique des signatures électroniques émanant de pays tiers, la Commission peut, le cas échéant, présenter des propositions visant à l'instauration effective de normes et d'accords internationaux applicables aux services de certification. Elle peut notamment, si besoin est, soumettre au Conseil des propositions concernant des mandats de négociation d'accords bilatéraux et multilatéraux avec des pays tiers et des organisations internationales. Le Conseil statue à la majorité qualifiée.

---

11 JO L 95 du 21.4.1993, p. 29.

Article 8
Protection des données

1. Les États membres veillent à ce que les prestataires de service de certification et les organismes nationaux responsables de l'accréditation ou de la supervision satisfassent aux exigences prévues par les directives du Parlement européen et du Conseil 95/46/CE[12] et 97/66/CE[13].

2. Les États membres veillent à ce qu'un prestataire de service de certification ne puisse recueillir des données personnelles que directement auprès de la personne qui fait l'objet des données et uniquement dans la mesure où cela est nécessaire à la délivrance d'un certificat. Les données ne peuvent être recueillies ou traitées à d'autres fins sans le consentement de la personne qui en fait l'objet.

3. Les États membres veillent à ce que, à la demande du signataire, le prestataire de service de certification indique dans le certificat un pseudonyme au lieu du nom du signataire.

4. Dans le cas de personnes utilisant un pseudonyme, les États membres veillent à ce que le prestataire de service de certification transmette les données concernant l'identité de ces personnes avec leur consentement aux pouvoirs publics qui en font la demande. Si la législation nationale exige, aux fins d'une enquête pénale concernant l'utilisation de la signature électronique sous un pseudonyme, de transférer les données révélant l'identité de la personne qui en fait l'objet, le transfert est consigné et la personne faisant l'objet des données est informée du transfert des données la concernant dans les meilleurs délais après la conclusion de l'enquête.

Article 9
Comité

La Commission est assistée par un comité de caractère consultatif dénommé "comité des signatures électroniques" (ci-après "le comité") composé des représentants des États membres et présidé par le représentant de la Commission.

Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause, le cas échéant en procédant à un vote.

L'avis est inscrit au procès-verbal; en outre, chaque État membre a le droit de demander que sa position figure à ce procès-verbal.

La Commission tient le plus grand compte de l'avis émis par le comité. Elle informe le comité de la façon dont elle a tenu compte de cet avis.

---

12 JO L 281 du 23.11.1995, p. 31.

13 JO L 24 du 30.1.1998, p. 1.

Article 10
Consultation du comité

Le comité est consulté, si besoin est, sur les exigences applicables aux prestataires de service de certification prévues à l'annexe II, et sur les normes généralement admises pour les produits de signature électronique conformément à l'article 3 paragraphe 3.

Article 11
Notification

1. Les États membres communiquent à la Commission les informations suivantes:

   a) des informations sur les régimes volontaires d'accréditation, ainsi que toute exigence supplémentaire visée à l'article 3 paragraphe 4;

   b) les noms et adresses des organismes nationaux responsables de l'accréditation et de la supervision; et

   c) les noms et adresses des prestataires de service de certification nationaux accrédités.

2. Les informations fournies en application du paragraphe 1 et les changements concernant ces informations sont notifiés dans les meilleurs délais par les Etats membres.

Article 12
Réexamen

1. La Commission examine le fonctionnement de la présente directive et présente un rapport sur ce point au Parlement européen et au Conseil au plus tard le 31 décembre 2002.

2. Le réexamen doit permettre, entre autres, de déterminer s'il convient de modifier le champ d'application de la directive pour tenir compte des progrès techniques et des changements juridiques. Le rapport doit notamment comporter une évaluation, fondée sur l'expérience acquise, des aspects relatifs à l'harmonisation. Il est accompagné, le cas échéant, de propositions législatives complémentaires.

Article 13
Mise en œuvre

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 31 décembre 2000. Ils en informent immédiatement la Commission.

   Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive et dans les domaines annexes, ainsi qu'un tableau de correspondance entre la présente directive et les dispositions adoptées pour sa publication.

Article 14
Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel des Communautés européennes*.

Article 15
Destinataires

Les États membres sont destinataires de la présente directive.

Fait à

Par le Parlement européen

Le Président

Par le Conseil

Le Président

Annexe I - Exigences concernant les certificats agréés

Tout certificat agréé doit comporter:

(a) l'identification du prestataire de service de certification qui délivre le certificat;

(b) le nom indiscutable du titulaire ou un pseudonyme ne prêtant pas à confusion et identifié comme tel;

(c) un attribut spécifique au titulaire déterminant, par exemple, son adresse, s'il est mandaté pour agir au nom d'une entreprise, s'il est solvable, s'il a un numéro de TVA ou d'identification fiscale, s'il a des garants ou s'il est titulaire de permis ou de licences particuliers;

(d) un dispositif de vérification de signature qui corresponde au dispositif de création de signature sous le contrôle du titulaire;

(e) l'indication du début et de la fin de la période d'effet du certificat;

(f) le code d'identification unique du certificat;

(g) la signature électronique du prestataire de service de certification qui délivre le certificat;

(h) les limites à l'utilisation du certificat, le cas échéant; et

(i) les limites à la responsabilité du prestataire de service de certification et la valeur des transactions pour lesquelles le certificat est valable, le cas échéant.

Annexe II - Exigences concernant les prestataires de service de certification

Les prestataires de service de certification doivent:

(a) démontrer qu'ils jouissent du crédit nécessaire pour offrir des services de certification,

(b) assurer un service de révocation rapide et sûr;

(c) vérifier, par des moyens appropriés, l'identité et les moyens d'action de la personne à laquelle un certificat agréé est délivré;

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

(e) utiliser des systèmes fiables et des produits de signature électronique qui assurent une protection contre toute modification non autorisée desdits produits pour qu'ils ne puissent être utilisés à des fins autres que celles pour lesquelles ils ont été conçus; ils doivent également utiliser des produits de signature électronique qui assurent la sécurité technique et cryptographique des processus de certification pris en charge par lesdits produits;

(f) prendre des mesures contre la contrefaçon des certificats et, au cas où le prestataire de service de certification génère des clés privées de signature cryptographique, garantir la confidentialité au cours du processus de génération desdites clés;

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

(h) enregistrer toutes les informations pertinentes concernant un certificat agréé pendant une période de temps appropriée, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques;

(i) ne pas stocker ou copier les clés privées de signature cryptographique de la personne à laquelle le prestataire de service de certification a offert des services de gestion de clés à moins que cette personne en ait fait explicitement la demande;

(j) informer les consommateurs, avant l'établissement de relations contractuelles, par écrit, dans une langue aisément compréhensible et par un moyen de communication durable, des conditions précises d'utilisation des certificats, y compris des limites de leur responsabilité, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges.

ISSN 0254-1491

COM(98) 297 final

DOCUMENTS

FR **15 06 10 01**

N° de catalogue : CB-CO-98-336-FR-C

ISBN 92-78-36441-X

Office des publications officielles des Communautés européennes

L-2985 Luxembourg