

procédures, pouvant aboutir à une suspension de 3 à 6 mois du régime de préférences tarifaires, contre ces pays. Un nouveau transfert de compétences en faveur de la Commission fait certes l'objet de réserves au sein du Comité, mais celles-ci sont reléguées au second plan compte tenu de l'accélération certaine des processus décisionnels qui en découlerait. Néanmoins, le Comité estime qu'il est urgent de protéger les intérêts élémentai-

res des entreprises importatrices par des mécanismes appropriés. Il recommande dès lors que les doutes éventuels en ce qui concerne l'usage régulier du système de préférences dans certains pays fassent le plus tôt possible l'objet d'une publication au Journal officiel des CE. Le cas échéant, les mesures mises en œuvre ne doivent en aucun cas porter atteinte aux contrats conclus avant cette publication, preuves à l'appui.

Bruxelles, le 2 décembre 1998.

La Présidente

du Comité économique et social

Beatrice RANGONI MACHIAVELLI

Avis du Comité économique et social sur la «Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques»

(1999/C 40/10)

Le 30 juillet 1998, le Conseil a décidé, conformément aux dispositions de l'article 100 A du Traité instituant la Communauté économique européenne, de consulter le Comité économique et social sur la proposition susmentionnée.

La section «Marché unique, production et consommation» chargée de préparer les travaux du Comité en la matière, a adopté son avis le 28 octobre 1998 (rapporteur: M. Burani).

Lors de sa 359^e session plénière des 2 et 3 décembre 1998 (séance du 2 décembre), le Comité économique et social a adopté à l'unanimité l'avis suivant.

1. Introduction

1.1. L'initiative de la Commission de présenter une proposition de directive sur le cadre normatif et juridique des signatures électroniques constitue la suite concrète de la communication intitulée «Assurer la sécurité et la confiance dans la communication électronique — Vers un cadre européen pour les signatures numériques et le chiffrement»⁽¹⁾.

1.2. Dans sa communication, la Commission relevait l'apparition d'une situation qui nécessite l'attention des autorités européennes: certains États membres ont adopté, ou sont en train d'adopter, des approches différentes en matière de réglementation des signatures électroniques. L'absence de reconnaissance mutuelle est susceptible de provoquer une fragmentation du marché intérieur du commerce électronique et des services en ligne dans l'Union européenne. Il est donc urgent de définir un cadre commun en respectant deux exigences principales: la création d'un cadre juridique précis et

une flexibilité suffisante pour éviter d'encadrer cette matière dans des systèmes qui ne répondent pas à la continuité de l'évolution de la technique.

1.3. Le Comité économique et social a souscrit aux considérations de la Commission⁽²⁾ en avançant des propositions en vue d'une approche réglementaire respectueuse des principes de l'autorégulation et de la subsidiarité dans les limites bien précises d'une législation commune minimale. Dans ses observations sur une communication ultérieure de la Commission sur «La mondialisation et la société de l'information — La nécessité de renforcer la coordination internationale»⁽³⁾, le Comité a par ailleurs relevé que l'harmonisation d'un cadre juridique européen avec le reste du monde — nécessaire si l'on veut garantir la sécurité du commerce électronique qui, vu sa nature, ne connaît pas de frontières — procède trop lentement, sous l'effet d'une gamme d'initiatives non coordonnées.

⁽¹⁾ COM(97) 503 final du 8.10.1997.

⁽²⁾ JO C 157 du 25.5.1998.

⁽³⁾ JO C 284 du 14.9.1998.

1.4. La décision de la Commission de présenter une proposition de directive constitue une initiative qui va dans le bon sens, surtout parce qu'elle est inspirée par la flexibilité nécessaire en vue d'une coordination internationale.

2. Observations générales

2.1. La signature électronique permet à celui qui reçoit des données transmises électroniquement de vérifier l'origine des données (authenticité) et de contrôler que les données originales sont complètes et inchangées (intégrité). La vérification de l'authenticité et de l'intégrité des données ne démontre pas nécessairement l'identité du signataire qui a généré les signatures électroniques, d'où la nécessité d'une confirmation par des tiers, appelés «prestataires de services de certification». L'utilisation du système de certification de la signature est par conséquent un moyen indispensable d'assurer la sécurité des parties contractantes et de développer la confiance dans le commerce électronique.

2.2. Afin d'assurer la reconnaissance mutuelle des principes de sécurité juridique à la base de la certification des signatures électroniques, la Commission s'est inspirée de concepts cohérents, vu l'évolution continue de la situation:

- la réglementation est neutre du point de vue technique et est ouverte à des moyens d'authentification autres que la cryptographie à clé publique; il a été tenu compte de la possibilité d'apparition de nouveaux systèmes;
- les États membres devraient éviter d'adopter des régimes d'autorisation préalable des prestataires de services de certification; d'autre part, il pourrait être utile d'adopter des régimes volontaires d'accréditation;
- la directive ne concerne que les signatures électroniques sur les messages échangés sur des réseaux ouverts; en ce qui concerne les réseaux fermés, il appartiendra à chaque prestataire de s'y conformer ou non;
- la nécessité de garantir la reconnaissance juridique des signatures électroniques suppose que soient précisées les exigences essentielles pour les prestataires de services, y compris leur responsabilité.

2.3. Le Comité souscrit à cette approche générale, qui s'inspire des principes d'un marché libre. Il estime cependant que la protection des utilisateurs n'a pas fait l'objet d'une attention suffisante. Il se réserve par conséquent le droit d'exprimer certaines observations ou suggestions dans le courant de l'analyse du document de la Commission.

2.4. S'agissant de l'insertion de la réglementation européenne dans un contexte mondial, la Commission relève que «de nombreuses activités et discussions sont en cours»⁽¹⁾; elle cite notamment les initiatives de la CNUDCI, de l'OCDE et de l'OMC. Comme le Comité l'a déjà fait remarquer⁽²⁾, ces initiatives — en soi louables — montrent que le risque existe concrètement d'un chevauchement des tâches entre les institutions et de double emplois — voire, pire, de contradictions — entre les différentes réglementations. En définitive, tout cela se traduit par des lenteurs bureaucratiques, des retards et des coûts pour le contribuable. Voulant tout faire et tout de suite, les institutions mondiales aboutissent à l'effet opposé, suscitant la confusion et l'incertitude. C'est avec regret que le Comité en prend acte.

3. Observations particulières sur la proposition de directive

3.1. Article 1

La directive a pour objet d'instituer un cadre juridique pour les services de certification accessibles au public, de faciliter l'utilisation des signatures électroniques et de garantir leur reconnaissance juridique. Elle ne couvre pas les aspects liés à la conclusion et à la validité des contrats. Compte tenu du libellé de cet article et des précisions du dixième «considérant», la portée de la directive est limitée aux systèmes ouverts; pour les systèmes fermés, la Commission laisse les parties libres de convenir entre elles des conditions auxquelles les signatures électroniques sont acceptées et reconnues.

3.1.1. Le Comité exprime quelques doutes à cet égard: si, d'une part, cette approche qui respecte la liberté contractuelle est louable, d'autre part, on ne peut ignorer que certains systèmes fermés sont ouverts à un public toujours plus nombreux qui n'est pas toujours et pas nécessairement au courant des règles de chaque système. Il est vrai qu'un système fermé a toujours la possibilité de se soumettre aux règles de la directive, mais le Comité se demande s'il ne serait pas plus sage — dans l'intérêt même des utilisateurs et des gestionnaires de systèmes fermés — d'étendre la portée de la directive aux systèmes fermés ouverts au public.

3.2. Article 3, paragraphes 1 et 2

Il est interdit aux États membres de soumettre la fourniture de services de certification à un régime d'autorisation préalable; ils peuvent toutefois instaurer ou maintenir des régimes volontaires d'accréditation sans toutefois limiter le nombre de prestataires de services.

⁽¹⁾ COM(1998) 297 final, point 7.

⁽²⁾ JO C 284 du 14.9.1998.

3.2.1. Le Comité propose d'accorder une attention particulière à la portée de ces dispositions. La fonction de certification est pourvue de validité non seulement entre les parties mais également, si nécessaire, vis-à-vis d'un tiers. Étant bien entendu que la demande d'accréditation reste un acte «volontaire», il faudrait prévoir la possibilité de distinguer clairement, comme nous le précisons plus loin, les actes certifiés par des prestataires accrédités et non accrédités. L'article 5, paragraphe 2, devrait stipuler avec précision que la validité des signatures électroniques, admises comme preuves en justice (procédures judiciaires et extra-judiciaires), n'est opposable aux tiers que lorsqu'elle repose sur un certificat délivré par un prestataire accrédité.

3.2.2. La situation existant aujourd'hui ne présente pas de motifs particuliers de préoccupation; toutefois, une législation ne saurait faire fi des évolutions imprévisibles qui surviendront à l'avenir: les quelques prestataires actuels, qui sont bien connus, pourraient se multiplier en conséquence d'une «banalisation» possible des techniques d'authentification. S'il est acceptable que le nombre de certificateurs ne soit pas limité, il n'est en revanche pas souhaitable qu'ils soient exemptés d'un contrôle préalable et d'une accréditation. Dans l'intérêt des utilisateurs et des tiers, il semblerait donc nécessaire d'établir que les «exigences concernant les prestataires de services de certification» énumérées à l'annexe II soient contrôlées par un pouvoir public lorsque ces prestataires agissent dans des systèmes ouverts ou dans des systèmes fermés ouverts au public.

3.2.3. L'accréditation des prestataires sous la responsabilité des pouvoirs publics devrait se baser sur le respect des exigences prévues à l'annexe II. Cette condition est nécessaire mais pas suffisante: il faut également s'assurer que ces exigences continuent à être respectées en prescrivant une supervision périodique. Les pouvoirs publics ne peuvent éluder leurs responsabilités: une fois la réglementation adoptée, ils doivent en garantir le respect.

3.3. Article 3, paragraphe 4

Cette disposition reconnaît aux États membres la possibilité d'admettre l'usage des signatures électroniques dans le secteur public sous réserve d'exigences supplémentaires.

3.3.1. Le Comité est d'accord avec cette disposition, mais se demande s'il ne conviendrait pas d'aller plus loin en imposant l'acceptation de la signature électronique dans le secteur public des États membres qui en reconnaissent la validité dans le secteur privé. Si les pouvoirs publics — qui ont pour tâche de garantir la sécurité des dispositifs juridiques et de protéger leurs citoyens — prennent la responsabilité de reconnaître la validité juridique d'une signature électronique dans les actes passés entre des particuliers, on ne voit pas

pourquoi la même attitude ne devrait pas également être adoptée pour les actes passés avec l'administration publique, éventuellement en introduisant des «exigences supplémentaires».

3.4. Article 4

Relatif au respect des règles du marché intérieur, cet article établit que les États membres ne peuvent imposer de restrictions à la fourniture de services de certification provenant d'autres États membres.

3.4.1. Le Comité fait observer que cette règle est certainement cohérente avec les principes du marché intérieur, mais qu'elle ne protège pas le public contre la prestation de services par des opérateurs non accrédités d'autres pays membres: s'il est déjà difficile pour un utilisateur de distinguer entre opérateurs accrédités et non accrédités de son propre pays, ce l'est davantage encore lorsque le fournisseur réside dans un pays tiers. Il existe dans ce cas une analogie notoire avec l'approche de la deuxième directive bancaire: la liberté de prestation de services s'applique uniquement aux institutions soumises à la directive. Pour les autres institutions, la prestation de services (financiers) reste limitée au pays d'origine.

3.4.2. Dans le cas qui nous occupe, étant donné la liberté de circulation des produits de signature électronique, leur admissibilité dans les procédures judiciaires et extra-judiciaires ne devrait être reconnue que lorsque la certification est délivrée par un opérateur accrédité.

3.5. Article 5

Les États membres doivent introduire dans leur législation des règles qui rendent impossible de contester la force exécutoire, les effets ou la validité juridique d'une signature électronique au seul motif que celle-ci se présente sous forme électronique ou qu'elle ne repose pas sur un certificat accrédité. Par ailleurs, ils doivent veiller à ce que les signatures certifiées par un prestataire accrédité aient la même valeur juridique que les signatures manuscrites et qu'elles soient admises comme preuve en justice.

3.5.1. Le Comité attire l'attention de la Commission sur une considération qui devrait renforcer la validité des observations formulées aux paragraphes 3.4.1 et 3.4.2: la seule différence entre des signatures certifiées par des opérateurs accrédités et par des opérateurs non accrédités réside dans la valeur probatoire de la certification. À cet égard, l'article 5, paragraphe 2, manque de clarté et mériterait d'être revu: d'après son libellé, les États membres devraient admettre comme preuve en justice les certificats délivrés par un prestataire «qui satisfait aux exigences prévues à l'annexe II». Une telle formulation laisse à penser que n'importe quel prestataire, à partir du moment où il satisfait aux

exigences prévues à l'annexe II, peut délivrer des certificats ayant une validité juridique. Si tel n'est pas le cas, le texte actuel doit être remplacé par la formule non équivoque «prestataire accrédité».

3.5.2. En outre — parallèlement aux observations formulées au paragraphe 3.4.2 —, la proposition est muette quant à la valeur probatoire d'une certification octroyée par un opérateur accrédité dans un pays tiers: dans ce cas également, la directive devrait contenir des dispositions précises. Pour sa part, le Comité propose qu'une certification de ce type soit admise à condition que le pays tiers accorde des conditions de réciprocité aux certificats de résidents de l'Union européenne.

3.6. Article 6

En matière de responsabilité, cet article prescrit une série d'obligations au prestataire de services de certification: exactitude des informations, conformité aux exigences de la directive, vérification de l'aptitude du titulaire et du certificateur en termes d'exigences techniques et technologiques. Il établit également les exemptions de responsabilité admises en cas d'erreurs contenues dans les informations originales et la possibilité d'établir des limites à la certification, tant sur le plan de son utilisation que du montant certifié.

3.6.1. Le Comité estime que les dispositions de cet article sont conformes aux principes généraux du droit et à celui de la liberté contractuelle. En même temps, il souhaite faire part d'une réflexion, ou plutôt d'une interrogation: en cas d'interruption ou de cessation du service par le prestataire de services de certification, quelles sont les responsabilités de ce dernier et de quelles garanties jouit l'utilisateur? Il conviendrait qu'existe un système ou un autre garantissant la continuité de la protection des droits des utilisateurs, par exemple au moyen d'une obligation de déposer une copie des dossiers auprès de tiers offrant des garanties déterminées.

3.7. Article 7, paragraphe 1

Cette disposition contient des prescriptions relatives aux fournisseurs résidant dans des pays tiers. Les certificats qu'ils fournissent seront reconnus comme juridiquement équivalents aux certificats européens si le prestataire a été accrédité dans un État membre dans le cadre du régime volontaire d'accréditation existant dans ce pays, ou si le certificat est garanti par un prestataire établi dans un État membre, ou encore si le certificat ou le prestataire est reconnu dans le cadre d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.

3.7.1. Le Comité est globalement opposé à cette disposition. Au nom de la liberté des échanges, elle ignore les principes de réciprocité qui devraient être à la base d'une intégration globale du commerce, électronique et autre. Les orientations exposées dans ce paragra-

phe — en particulier celles relatives à l'accréditation dans un pays membre d'un prestataire étranger et à la garantie donnée par un prestataire européen à un certificat émis par un pays tiers — sont acceptables à condition que le pays tiers octroie un traitement analogue ou équivalent aux prestataires ou aux certificats provenant de l'ensemble des pays membres.

3.7.2. S'agissant de la reconnaissance d'un certificat ou d'un prestataire d'un pays tiers sur la base d'un accord bilatéral avec un pays membre, le Comité observe que l'adoption de ce principe équivaut à introduire des distorsions de concurrence entre pays membres, plus précisément entre pays dotés de réglementations plus «libérales» et les autres. La libre prestation de services ne peut être utilisée comme cheval de Troie pour introduire des opérateurs ou des produits de pays tiers dans l'Union européenne par le biais d'un accord bilatéral avec un seul pays membre.

3.7.3. Il ne sert à rien, pour défendre la thèse opposée, d'invoquer certains précédents tels que celui de la deuxième directive bancaire: dans ce cas, le pays «hôte» exerce une surveillance continue et garantit la solidité et la solvabilité de l'entreprise du pays tiers, qui doit en tout état de cause être physiquement présente sur son territoire; ces conditions sont bien loin d'être satisfaites dans le cas des garanties relatives aux signatures électroniques.

3.8. Article 8

Les règles évoquées dans cet article n'appellent pas d'observations particulières, à l'exception de celles du paragraphe 4 relatives à l'utilisation de pseudonymes. Le prestataire de service doit pouvoir transmettre les données concernant l'identité du titulaire du pseudonyme aux pouvoirs publics qui en font la demande, moyennant le consentement préalable du titulaire lui-même. En outre, la directive n'apporte pas de réponse à la question de savoir quelle serait la position du prestataire au cas où le titulaire ne consentirait pas à ce que son identité soit révélée aux autorités.

3.8.1. La deuxième partie du même paragraphe suscite d'autres doutes: si la législation nationale exige — aux fins d'une enquête concernant des infractions à l'utilisation de la signature électronique sous un pseudonyme — que le prestataire transfère les données révélant l'identité de la personne qui en fait l'objet, celle-ci n'est informée de cette transmission qu'après la conclusion de l'enquête.

3.8.2. Le Comité s'interroge quant à l'opportunité d'entrer dans ces détails: une fois l'enquête conclue, l'intéressé saura déjà que ses données ont été révélées, cette disposition apparaissant dès lors inutile. Il souligne par ailleurs que lorsqu'il est question de «législation nationale», il conviendrait de clairement spécifier de quelle législation nationale il s'agit: de celle du pays du prestataire de services — comme on peut le présumer — ou de celle du pays du titulaire du pseudonyme (à

supposer qu'elle soit connue), ou encore de l'autorité d'un autre pays membre. Vu que nous nous trouvons — de toute évidence même si ce n'est pas explicite — dans le domaine de la lutte contre la criminalité, la directive devrait être plus précise en ce qui concerne les procédures à suivre et les droits et les obligations du prestataire de services.

3.8.3. Tout bien considéré, le CES se demande s'il ne faudrait pas revoir l'ensemble du texte de cet article et prévoir l'application intégrale des dispositions contenues dans les directives pour la protection des données personnelles et contre le blanchiment de capitaux: en définitive, il n'existe pas de différence entre les transactions sur papier et les transactions électroniques.

3.9. *Articles 9 et 10*

Ces articles prévoient l'institution d'un «comité des signatures électroniques» composé de représentants des États membres et présidé par la Commission. Il est consulté sur les exigences applicables aux prestataires de services et sur les normes admises pour la production de signatures électroniques. Ce comité est informé par la Commission des résultats des rencontres périodiques entre celle-ci et les entreprises, les utilisateurs et les consommateurs.

3.9.1. Le Comité prend acte de cette initiative, mais se demande s'il est vraiment nécessaire d'instituer un comité alors que la Commission elle-même, dans le cadre de ses fonctions institutionnelles, pourrait aisément consulter les États membres et les parties intéressées

sans avoir besoin d'une interface qui, en définitive, fait double emploi avec les compétences de la Commission. Il s'agit avant tout d'une procédure normale au sein de la Commission: le Comité ne voit pas la nécessité d'un alourdissement bureaucratique qui n'apporterait rien en termes d'efficacité.

3.10. *Articles 12 et 13*

Les dispositions de ces deux articles — dont l'ordre semble inversé, en termes de séquence temporelle et logique — prévoit que les États membres doivent se conformer à la directive au plus tard le 31 décembre 2000, et que la Commission rendra compte pour la première fois de sa mise en œuvre effective au Parlement européen et au Conseil au plus tard le 31 décembre 2002. Le Comité a souligné à plus d'une occasion ⁽¹⁾ le caractère urgent de l'adoption d'une législation uniforme dans le vaste domaine de la société de l'information; il se demande s'il est vraiment nécessaire de laisser si longtemps aux États membres pour se conformer à la directive vu que plusieurs d'entre eux ont fait preuve d'une grande diligence pour adopter très rapidement leur propre législation. L'introduction de mesures d'harmonisation — peu nombreuses en vérité — ne devrait pas nécessiter d'efforts excessifs ni de longs délais aux législateurs nationaux. Une période d'un an à compter de la date d'adoption de la directive semble suffisante au Comité pour apporter des modifications éventuelles — et modestes — aux législations existantes ou pour rédiger de nouveaux textes.

⁽¹⁾ JO C 284 du 14.9.1998, JO C 157 du 25.5.1998, JO C 19 du 21.1.1998.

Bruxelles, le 2 décembre 1998.

La Présidente

du Comité économique et social

Beatrice RANGONI MACHIAVELLI