

Avis du Comité économique et social sur la
« Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions
:
Assurer la sécurité et la confiance dans la communication électronique
—
Vers un cadre européen pour les signatures numériques et le chiffrement »

(98/C 157/01)

Le 10 octobre 1997, la Commission a décidé, conformément aux dispositions de l'article 198 du Traité instituant la Communauté européenne, de saisir le Comité économique et social d'une demande d'avis sur la communication susmentionnée.

La section de l'industrie, du commerce, de l'artisanat et des services, chargée de préparer les travaux du Comité en la matière, a émis son avis le 4 mars 1998 (rapporteur: M. Burani).

Au cours de sa 353e session plénière des 25 et 26 mars 1998 (séance du 25 mars), le Comité économique et social a adopté par 101 voix pour, 1 voix contre et 1 abstention l'avis suivant.

1. Observations générales

- 1.1. La Communication de la Commission constitue une tentative réussie de créer un cadre réglementaire pour la communication électronique, matière hautement technique et spécialisée. La compréhension des aspects techniques est par ailleurs nécessaire pour les utilisateurs, mais surtout pour les autorités publiques et les législateurs.
- 1.2. La communication électronique sur des réseaux ouverts, tels qu'Internet, prend une ampleur encore inconcevable il y a dix ans, et son développement futur constituera probablement l'une des caractéristiques essentielles de la société de la fin de ce millénaire et du début du prochain millénaire. Les perspectives qui se dessinent pour le proche avenir sont celles d'une croissance exponentielle; cependant, les applications pratiques dans les différents secteurs d'activité et en particulier dans le domaine du commerce électronique () dépendront de la capacité à lever les obstacles à un développement harmonieux de la communication électronique.
- 1.3. La Commission considère que ces obstacles tiennent aux incertitudes inhérentes à l'utilisation de réseaux ouverts: les messages peuvent être interceptés et manipulés, la validité des documents peut être contestée, les données personnelles peuvent être recueillies de manière illicite, les communications peuvent être utilisées à des fins illégales. Il est donc nécessaire de créer une infrastructure sûre permettant d'une part l'instauration d'une société de l'information qui protège les citoyens contre les abus et d'autre part le développement d'un commerce électronique reposant sur des bases au moins aussi fiables que celles sur lesquelles s'effectuent aujourd'hui les échanges de documents papier dans les milieux économiques.
- 1.4. Le document à l'examen traite de deux outils fondamentaux pour l'obtention de cette fiabilité: la signature numérique et le chiffrement; la première garantit l'identité des parties au contrat et l'origine des messages (authenticité), le second protège contre les intrusions indues (intégrité) et assure la confidentialité des communications. La Commission veut offrir des garanties de sécurité, avec le concours de tous les partenaires intéressés, en ce qui concerne la situation actuelle et son évolution possible. Le CES s'en félicite et demande à être consulté sur les initiatives futures de la Commission.
- 1.5. Le Parlement européen et le Conseil des ministres ont demandé à la Commission de prendre les dispositions adéquates pour la mise en oeuvre de mesures à même de garantir l'intégrité et l'authenticité des documents électroniques. Le CES fait observer que l'on ne saurait en tout état de cause faire abstraction des autres initiatives, en cours ou déjà adoptées, émanant de pays tiers et d'organisations internationales (OCDE, CNUDCI, etc.).
- 1.6. Le CES relève également que la réglementation de cette matière devrait être entreprise à partir d'une vision d'ensemble claire : d'une part, il faudra procéder avec flexibilité afin de ne pas entraver les progrès technologiques et leurs applications; d'autre part, il conviendra de préserver les principes fondamentaux de l'UE: protection des consommateurs, égalité des conditions de concurrence, libre circulation des services, reconnaissance mutuelle. La communication électronique constitue une révolution de portée au moins égale à la révolution industrielle du siècle dernier: le cadre juridique et réglementaire doit porter l'empreinte de concepts novateurs fondés sur les progrès déjà réalisés et sur des prévisions raisonnables pour l'avenir.
- 1.7. La législation existante, qui a évolué pendant deux millénaires à partir du droit romain, est fondée sur des documents papier; ceux-ci sont destinés à être remplacés dans un avenir proche - dans une mesure encore impossible à évaluer, mais certainement importante - par des «documents» électroniques. Il s'agit d'un changement radical qui exige une approche différente de la question de la validité des contrats, mais aussi de celle de la validité de la documentation électronique échangée entre particuliers et entre ceux-ci et l'administration publique (impôts, sécurité sociale, enregistrement d'actes, justice, etc.).

- 1.8. L'administration publique a déjà recours dans différents pays à la communication électronique pour l'échange d'informations et de documents en son sein et dans ses rapports avec les citoyens. Une fois mis en place un cadre juridique et réglementaire sûr, la communication électronique devra également pouvoir s'appliquer aux actes juridiquement et administrativement importants: une révolution d'une portée peut-être encore supérieure à celle qui doit intervenir dans le domaine du droit privé.
- 1.9. Il est donc nécessaire d'instaurer un nouveau cadre législatif et réglementaire fondé sur l'immatérialité de la documentation. Le secteur du droit privé et administratif relève en grande partie de la compétence des États membres; différentes initiatives ont en effet été adoptées ou sont à l'étude. Une première analyse sommaire amène à constater que les orientations et les solutions adoptées divergent souvent sensiblement. Le CES attire l'attention de la Commission et des États membres sur l'impérieuse nécessité de parvenir de toute urgence à une harmonisation au niveau européen des principes de base. Les exigences de fonctionnement du marché unique mettraient rapidement en évidence les graves inconvénients inhérents à des infrastructures juridiques et réglementaires différentes selon les pays. Une harmonisation a posteriori serait extrêmement difficile.

2. Introduction: Le besoin de communications électroniques sécurisées ()

- 2.1. Le CES a pris connaissance des aspects techniques de la communication électronique, de la signature numérique et du chiffrement. Il félicite la Commission d'avoir traité une matière aussi complexe et spécialisée en la rendant accessible à un public ne possédant pas nécessairement les connaissances scientifiques nécessaires. Le Comité n'entend pas entrer dans le détail de ces questions; ses commentaires se limitent donc aux particularités opérationnelles et fonctionnelles pouvant nécessiter une intervention réglementaire ou législative de la part des institutions européennes.
- 2.2. Étant donné l'impossibilité d'assurer une sécurité absolue et totale en matière de communication électronique, le Comité rappelle que le principal danger existant dans ce domaine est la fraude, sous ses différentes formes et applications; il est incontestable que de ce point de vue, les réseaux ouverts (du type Internet) sont vulnérables, du moins tant que n'auront pas été prises sur une grande échelle des mesures de sécurité efficaces. La Commission rappelle à ce propos que les documents importants sont échangés sur des réseaux fermés, dont l'accès est réservé à des utilisateurs se connaissant déjà et liés par des rapports de confiance réciproque.
- 2.3. Les réseaux fermés, tout à fait légitimes, se sont développés indépendamment des réseaux ouverts, grâce à leurs propres systèmes de communication ou via Internet. Du point de vue de leurs avantages respectifs, l'utilisation des réseaux fermés est probablement plus coûteuse que celle des réseaux ouverts, mais l'élément déterminant du choix est certainement la sécurité comparativement supérieure des premiers par rapport aux seconds. Leur développement sera donc fonction de la fiabilité des réseaux ouverts: plus cette dernière sera grande, moins il y aura de raisons de créer de nouveaux réseaux fermés. Au nom de la liberté contractuelle, le CES ne voit pas la nécessité de réglementer ce secteur; néanmoins, les doutes concernant la validité de l'authentification des opérations réalisées avec des tiers, dans l'hypothèse où elles ne seraient pas reconnues et approuvées par une autorité de certification (voir plus loin, paragraphe 5), pourraient poser un problème.
- 2.4. L'objectif général de la Communication n'est du reste pas de traiter la question de la sécurité en tant que telle; il est en fait beaucoup plus vaste et ambitieux, puisqu'il vise à:
- établir un cadre européen de la signature numérique;
 - assurer le fonctionnement du marché unique pour les produits et services cryptographiques;
 - résoudre les problèmes internationaux liés à la nature universelle d'Internet;
 - intégrer le chiffrement dans les autres politiques européennes;
 - permettre aux utilisateurs de bénéficier des possibilités offertes par la société de l'information, qualifiée par la Commission de «planétaire».
- 2.5. Ce cadre d'action est approuvé par le Comité. Celui-ci attire par ailleurs l'attention sur un aspect qui peut sembler évident mais qui est parfois négligé au fil des travaux: la nécessité pour toute initiative européenne de tenir compte du caractère «planétaire» de la communication électronique: le désir de faire plus et mieux que les autres peut entraîner l'application préjudiciable de critères divergents. La Commission semble avoir suivi cette approche; le Comité souligne pour sa part que l'Europe devrait si possible et dès que possible prendre la direction des initiatives, sans perdre de vue ce que les autres font ou ont fait. La coopération internationale () en cours ou programmée a donné de bons résultats, mais les mécanismes de décision impliquent de longs délais, alors qu'une réglementation européenne est nécessaire au plus tôt. Celle-ci devrait donc être suffisamment flexible pour en permettre l'adaptation aux exigences des relations internationales.

3. Authentification et intégrité: Les signatures numériques ()

- 3.1. La signature numérique garantit que le message provient d'une personne identifiée et autorisée (authenticité) et que lors de la transmission, son contenu n'a pas été altéré par des tiers ou de manière accidentelle (intégrité) (). La signature numérique est fondée sur un système cryptographique utilisant une clé publique (connue de tous les utilisateurs d'un système donné) et une clé privée (connue seulement par l'expéditeur).
- 3.2. Une signature numérique sûre (ainsi que d'autres systèmes alternatifs en cours d'expérimentation) est la condition indispensable de 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 des transactions conclues par voie de communication électronique.
- 3.3. Dans les systèmes fermés, la validité des contrats conclus entre les participants ne pose pas de problèmes, puisque la confiance réciproque - fondée sur la rigueur des conditions d'accès, la transparence des critères de sécurité et la liberté contractuelle - est le fondement même de la création de ces systèmes. Parmi les différentes techniques adoptées, il est bon de rappeler que le protocole SET (Secure Electronic Transaction) () a été créé dans le domaine des services financiers appliqués au commerce électronique. Il est accessible au moyen d'un certificat électronique (digital certificate) aux titulaires de cartes de paiement, aux détenteurs de monnaie électronique, aux acheteurs de marchandises ou de services auprès d'opérateurs affiliés à ce système. Il faut d'ailleurs signaler qu'en toute rigueur, SET ne peut être défini comme un «système fermé», mais comme un «système ouvert payant».
- 3.4. Il y a lieu d'assurer la reconnaissance juridique de la validité des contrats conclus sur des réseaux ouverts, tant pour ce qui est des rapports entre les parties contractantes qu'avec des tiers. Certaines juridictions nationales reconnaissent déjà la validité de la signature numérique, mais seule une législation supranationale harmonisée peut garantir le développement du commerce électronique à l'échelle mondiale.

4. Les communications électroniques confidentielles: Le chiffrement ()

- 4.1 Outre l'authenticité et l'intégrité du message (voir paragraphes 1.4 et 3.1), les communications électroniques nécessitent, à l'instar des communications écrites, une confidentialité; cette exigence, importante sur les réseaux fermés, devient vitale sur les réseaux ouverts. Le chiffrement garantit que le message ne soit pas compréhensible par des tiers autres que l'expéditeur et le destinataire.
- 4.2 Le principe de base du système cryptographique est que seul l'expéditeur peut crypter le message et que seul le destinataire peut le déchiffrer. D'après le document de la Commission, il existe dans le commerce de nombreux produits cryptographiques «préfabriqués», en 1 400 versions différentes. Pour qu'un échange de messages cryptés et déchiffrables soit possible, il faut bien entendu que l'expéditeur et le destinataire soient en possession de logiciels compatibles.
- 4.4. La prolifération des systèmes de cryptage complique la gestion du logiciel par les individus dans leurs rapports avec une pluralité de parties. Cela mis à part, le cryptage en soi soulève des problèmes de fond d'une extrême importance. En premier lieu, les principes fondamentaux de la protection de la vie privée (ainsi que des droits d'auteur et de la protection du secret industriel) et de la protection du monde économique contre les intrusions illégales impliquent que les utilisateurs puissent se servir d'un système de chiffrement assurant un degré élevé de confidentialité des communications. En second lieu, il faut protéger la collectivité contre les utilisations illicites, telles que l'espionnage, le terrorisme, les activités criminelles ou en tout cas illégales.
- 4.4. Il résulte de ce qui précède qu'il est nécessaire de procéder à une réglementation de ce domaine, laquelle doit être harmonisée entre les États membres à partir de principes communs. Elle devrait concilier - dans la mesure du possible - des exigences apparemment opposées. Le Comité souligne que tout citoyen devrait avoir le droit d'accéder à des systèmes de chiffrement, mais il reconnaît que ce droit devrait être limité par la nécessité de la société de se protéger contre les activités criminelles ou illicites de toutes natures. La difficulté consiste à définir cette limite, qui peut varier d'un pays à l'autre mais aussi dans le temps, suivant la situation politique et sociale d'un pays. Il est clair que ce problème ne peut être résolu que par chaque État membre, selon des principes d'équité et de proportionnalité. L'autre problème à résoudre est celui de la détermination des cas dans lesquels les droits du citoyen ne s'appliquent pas et celle des modalités d'intervention des autorités, le tout dans le cadre d'une sécurité juridique donnant des garanties aux citoyens quant à l'utilisation des informations recueillies.

5. Les autorités de certification (AC) et les tiers de confiance (TC) ()

- 5.1. L'ensemble des problèmes exposés plus haut impliquent l'existence de systèmes en mesure d'assurer la fiabilité maximale des signatures numériques et des systèmes de chiffrement, ainsi que l'échange des clés, leur certification, la confidentialité des messages et dans le même temps le respect des exigences de protection de la société contre la criminalité.
- 5.2. Le problème de l'instauration d'un cadre juridique concernant la reconnaissance du point de vue de tiers des actes transmis sur des réseaux ouverts par le biais de signatures numériques (et éventuellement cryptés) n'est pas encore réglé au niveau communautaire. La

Commission s'oriente vers l'instauration, dans chaque pays de l'UE, d'une ou plusieurs autorités de certification (AC) juridiquement reconnues, et qui en tant que telles feraient office de «notaire» dépositaire des clés publiques.

- 5.3. Une AC légalement reconnue remplirait donc des fonctions de droit public; par ailleurs, elle ne pourrait pas - ou ne devrait pas - remplir les fonctions accessoires et fournir les services qui sont propres aux TC, dont les activités sont d'ordre privé. Il convient donc, toujours selon la Commission, de bien distinguer et différencier ces deux types d'organismes. Le CES est d'accord avec cette approche. Il reste à décider s'il convient que les AC aient le statut d'établissements publics ou d'établissements privés munis d'une autorisation publique. L'important étant que leur rôle soit reconnu et réglementé, le CES considère que cette décision peut revenir à chaque État membre.
- 5.4. Le CES se demande en outre s'il est toujours et dans chaque cas nécessaire d'instituer des AC, ou tout au moins d'étendre leurs compétences à tous les systèmes existants. Dans certains cas, les participants à un système (par exemple SET) sont des centaines de milliers et seront bientôt des millions. Le dépôt et la gestion des différentes clés seraient extrêmement complexes et coûteux. La solution la plus simple et la moins coûteuse serait probablement de reconnaître juridiquement comme AC «privée» les TC offrant des garanties d'intégrité et d'expérience.

6. Observations finales

- 6.1. Le programme de la Commission, assez complexe, est bien structuré et le CES marque son accord de principe avec celui-ci. Pour éviter de revenir sur des considérations qu'il fait également siennes, il formule certaines observations susceptibles de contribuer aux réflexions en cours.
- 6.2. En matière d'interopérabilité (), la Commission encourage l'industrie et les organisations internationales de normalisation à développer des normes techniques et d'infrastructure afin d'assurer un usage sûr des réseaux. Elle étudie la possibilité d'adopter des mesures permettant de soutenir les travaux des entreprises européennes dans ce domaine. Le CES, tout en rappelant que la définition de normes a des répercussions sur la compétitivité de l'industrie européenne par rapport à celle de pays tiers, suggère que l'action de la Commission s'inscrive dans le cadre des mesures qu'elle a elle-même prévues dans sa «Communication sur la compétitivité des industries européennes liées aux technologies de l'information et des communications (3)(3) JO C 73 du 9.3.1998, p. 1.».
- 6.3. Il faudrait également développer une stratégie visant à favoriser l'utilisation des communications électroniques par les PME; outre les diverses mesures déjà suggérées par le Comité dans son avis sur le «commerce électronique» (), il serait utile de fournir aux PME des solutions «clé en main» telles que celles expérimentées avec le programme TEDIS. Les chambres de commerce et certaines organisations professionnelles pourraient contribuer de manière déterminante à la pénétration du secteur des nouvelles technologies. Parallèlement, il convient d'attirer l'attention sur la nécessité que les mesures de diffusion de la communication électronique s'accompagnent d'une campagne de sensibilisation des PME aux risques et aux coûts inhérents à l'utilisation de ces nouvelles techniques. Comme pour toute innovation, les décisions doivent être prises de manière responsable dans ce domaine également, en parfaite connaissance des aspects positifs et négatifs des choix opérés.
- 6.4. Il existe un autre aspect implicite de la Communication, mais non explicitement traité: celui de la protection des consommateurs et, plus généralement, de tous les participants à la communication électronique. Il s'agit d'un problème prioritaire, avec des facettes assez complexes sous l'angle du droit international. Les garanties relatives offertes par la signature numérique favoriseront les contrats négociés à distance. Alors que les dispositions européennes et les autres dispositions législatives nationales s'appliquent sans difficulté d'interprétation aux contrats conclus entre acheteurs et vendeurs d'un même pays, les contrats négociés entre des personnes résidant dans différents pays de l'UE peuvent susciter une certaine incertitude lorsque le niveau de protection n'est pas le même. La situation se complique encore lorsque l'acheteur ou le vendeur réside dans un pays tiers. Le Comité estime que les règles relatives à la validité des contrats conclus par voie électronique doivent faire l'objet d'un cadre juridique européen; il recommande par ailleurs de résister à toute tentation d'application extraterritoriale du droit, en s'opposant dans le même temps aux multiples tentatives faites dans cette direction par les autorités de pays tiers.
- 6.5. Les disparités existant en ce qui concerne le niveau de protection des consommateurs au niveau mondial (mais aussi entre les États membres de l'UE) ne seront pas éliminées à court terme: d'ici là, le consommateur, de même que tout autre utilisateur, devra être informé que la «protection européenne» ou «nationale» peut ne pas être assurée pour les contrats négociés avec des fournisseurs de pays tiers ou d'autres pays de l'UE. Les dispositions en matière de droits d'auteur, de droits civiques, de liberté d'opinion et de moralité (pornographie, etc.) appellent des commentaires similaires.
- 6.6. Les lois fiscales, particulièrement en matière de TVA, posent un problème délicat. En principe, on peut s'attendre à ce que tous les gouvernements s'opposent avec force à tout accord ou acte législatif entraînant une perte de recettes, ainsi qu'aux systèmes permettant de tourner aisément les dispositions fiscales. Le CES se demande si l'harmonisation projetée au niveau européen (), qui prévoit l'imputation de la TVA en fonction du lieu de résidence de l'acheteur est applicable au commerce électronique, surtout vis-à-vis de pays tiers.

- 6.7. La nature globale d'Internet ajoute une nouvelle dimension au problème de la fraude et de la lutte contre la criminalité organisée. Les lois pénales dans ce domaine diffèrent dans une mesure significative et font parfois carrément défaut. Parallèlement aux interventions de l'UE déjà programmées (), l'Europe devrait promouvoir des mesures énergiques d'harmonisation et de coopération internationale, non limitées aux pays les plus importants. Il conviendra également au sein de l'UE de fournir une assistance adéquate en matière de formation aux organismes - en particulier Europol - chargés de combattre la criminalité.
- 6.8. En conclusion, l'adoption des communications électroniques en remplacement des communications écrites nécessite un encadrement juridique et réglementaire extrêmement complexe impliquant une vaste gamme d'activités. Outre un programme d'initiatives, la Commission a établi un calendrier des actions à entreprendre: le Comité ne peut que se féliciter des bonnes intentions manifestées, mais il se demande s'il sera possible de respecter tous les délais fixés, en particulier ceux qui dépendent de la conclusion d'accords internationaux.
- 6.9. Il conviendrait enfin d'établir au préalable quelles sont les limites d'une intervention législative ou réglementaire de l'Union européenne ou des États membres. Le CES estime qu'en dehors des dispositions nécessaires pour donner des garanties juridiques aux contrats et supprimer les dispositions nationales faisant obstacle à l'interopérabilité, une large place devrait être laissée à l'autoréglementation (codes de conduite). Celle-ci devrait notamment porter sur la compatibilité des nouveaux systèmes avec ceux les ayant précédés, sur l'application des mêmes règles et normes de sécurité aux systèmes fermés et ouverts et sur l'égalité de conditions entre participants de pays différents. L'intervention des pouvoirs publics devrait se limiter au contrôle du fonctionnement des systèmes et de leur conformité aux principes généraux du marché intérieur.
- 6.10. D'un point de vue pratique, le Comité estime devoir présenter les suggestions suivantes comme lignes d'action pour les futures
- à relativement brève échéance, tous les citoyens devraient pouvoir disposer d'un moyen (carte bancaire, carte de sécurité sociale, etc.) leur permettant de signer par voie électronique. Cela suppose l'existence d'un numéro national personnalisé enregistré et, bien sûr, d'une banque de données centralisée;
 - les administrations publiques devraient au plus vite être en mesure de fournir et d'accepter des documents électroniques. L'accès pourrait s'effectuer, dans les premiers temps du moins, par le biais de terminaux installés auprès d'institutions publiques;
 - il y a lieu d'assurer la reconnaissance mutuelle, au niveau mondial, des autorités de certification;
 - la confidentialité de la correspondance est garantie par la plupart des constitutions des États démocratiques, les exceptions à cette règle étant définies par la loi. La communication électronique devrait être protégée de manière analogue et suivant les mêmes critères.

Bruxelles, le 25 mars 1998.

Le Président du Comité économique et social

Tom JENKINS

() JO C 19 du 21.1.1998, p. 72.

() Cf. Communication, chap. I, p. 1-3.

() Cf. Communication, chap. IV, point 1.2 (iii), p. 19.

() Cf. Communication, chap. II, p. 3-4.

() En ce qui concerne les aspects techniques - plutôt complexes - cf. la Communication et en particulier les annexes I et II.

() SET inclut, outre l'intégrité du message et l'authentification de la signature, le chiffrement de la communication (voir plus loin, paragraphe 5.2).

() Cf. Communication, chap. III, p. 11-13.

() Cf. Communication, chap. II, point 2, p. 4-5.

() Cf. Communication, chap. IV, point 3, p. 20-21.

() JO C 19 du 21.1.1998, p. 72.

() JO C 296 du 29.9.1997.

() JO C 251 du 15.8.1997.