

20 mai 1998

A4-0189/98

RAPPORT

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
(COM(97)0503 - C4-0648/97)

Commission juridique et des droits des citoyens

Rapporteur: M. Wolfgang Ullmann

Rapporteur pour avis :

M. W.G. van Velzen, commission économique, monétaire et de la politique industrielle (*)

(* Procédure HUGHES)

SOMMAIRE

Page

| | |
|---|----|
| Page réglementaire | 3 |
| A. PROPOSITION DE RÉOLUTION | 4 |
| B. EXPOSÉ DES MOTIFS | 9 |
| | |
| Avis de la commission économique, monétaire et de la politique industrielle (*) | 13 |
| Avis de la commission de la culture, de la jeunesse, de l'éducation et des médias | 19 |

(* Procédure HUGHES)

Par lettre du 9 octobre 1997, la Commission a transmis au Parlement européen une communication au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions intitulée "Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et le chiffrement" (COM(97)0503 - C4-0648/97).

Au cours de la séance du 15 décembre 1997, le Président du Parlement a annoncé qu'il avait renvoyé cette communication, pour examen au fond, à la commission juridique et des droits des citoyens et, pour avis, à la commission économique, monétaire et de la politique industrielle, à la commission de l'environnement, de la santé publique et de la protection des consommateurs et à la commission de la culture, de la jeunesse, de l'éducation et des médias.

Au cours de sa réunion du 27 novembre 1997, la commission juridique et des droits des citoyens avait nommé M. Ullmann rapporteur.

Au cours de la séance du 13 mars 1998, le Président du Parlement européen a annoncé que le présent rapport devait être élaboré conformément à la procédure HUGHES par la commission juridique et des droits des citoyens, en liaison avec la commission économique, monétaire et de la politique industrielle.

Elle a examiné la communication de la Commission et le projet de rapport au cours de ses réunions des 14 avril 1998 et 19 mai 1998.

Au cours de la dernière de ces réunions, elle a adopté la proposition de résolution à l'unanimité.

Étaient présents au moment du vote les députés : De Clercq, président; Malangré, vice-président; Ullmann, rapporteur; Añoberos Trias de Bes (suppléant M. Casini C.), Barzanti, Berger, Buffetaut, Cassidy. Cot, Falconer (suppléant M. Martin D.), Gebhardt, Oddy, Thors et Verde i Aldea.

Les avis de la commission économique, monétaire et de la politique industrielle et de la commission de la culture, de la jeunesse, de l'éducation et des médias sont joints au présent rapport; la commission de l'environnement, de la santé publique et de la protection des consommateurs a décidé le 21 janvier 1998 qu'elle n'émettrait pas d'avis.

Le rapport a été déposé le 20 mai 1998.

Le délai de dépôt des amendements sera indiqué dans le projet d'ordre du jour de la période de session au cours de laquelle le rapport sera examiné.

A.
PROPOSITION DE RÉSOLUTION

Résolution 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" (COM(97)0503 - C4-0648/97)

Le Parlement européen,

- vu 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" (COM(97)0503 - C4-0648/97),
 - vu sa résolution du 19 septembre 1996 sur la recommandation au Conseil européen intitulée "L'Europe et la société de l'information planétaire" et sur la communication de la Commission intitulée "Vers la société de l'information en Europe: un plan d'action"⁽¹⁾,
 - vu les résultats de la conférence ministérielle européenne intitulée "Global Information Networks: Realising the Potential", qui a eu lieu les 6, 7 et 8 juillet 1997 à Bonn,
 - vu le rapport de la commission juridique et des droits des citoyens et les avis de la commission économique, monétaire et de la politique industrielle, et de la commission de la culture, de la jeunesse, de l'éducation et des médias (A4-0189/98),
- A. considérant que la communication électronique pose notamment trois problèmes: celui de l'authenticité de l'information, celui de l'intégrité de l'information communiquée et celui de la confidentialité de l'information,
- B. considérant que la nécessité de dispositions juridiques concernant l'authenticité de l'information a été reconnue dans tous les États membres de l'UE et que huit de ceux-ci ont déjà adopté ou sont occupés à élaborer des dispositions législatives,
- C. considérant que le commerce électronique et de nombreuses autres applications de la société de l'information ne se développeront que si la confidentialité peut être garantie de manière conviviale et à prix avantageux, mais que les autorités pénales et de sécurité craignent que la diffusion du recours à la communication chiffrée n'entrave la lutte contre la criminalité,
1. partage l'avis de la Commission selon lequel le commerce électronique est appelé à devenir un des moteurs du développement de la société de l'information planétaire; fait toutefois observer que les techniques abordées dans la communication de la Commission verront leur importance

⁽¹⁾ JO C 320 du 28.10.1996, p. 164, paragraphe 106 de la résolution.

s'accroître non seulement dans le domaine du commerce, mais aussi dans celui de la vie quotidienne des citoyens;

2. est d'avis que, en ce qui concerne le problème de l'authenticité et de l'intégrité de l'information, que les signatures numériques pourraient résoudre, il y a lieu de créer au niveau européen un cadre juridique assurant la confiance mutuelle à l'égard des signatures numériques et la confidentialité et favorisant le développement d'une offre diversifiée de certificats de nature à répondre aux différentes applications, notamment en matière de commerce électronique et de communication électronique entre les organes de l'État et le citoyen. Ce cadre juridique doit, à titre principal, viser à éliminer les contraintes imposées au plan national à l'activité de certification;
3. juge impératif que soient prises les mesures nécessaires pour éliminer les entraves à l'utilisation des signatures numériques dans les domaines juridique, économique et de l'administration publique; demande par conséquent, en particulier, l'égalité juridique entre signatures numériques et signatures traditionnelles;
4. engage les organes de l'Union européenne à jouer un rôle de fourrier dans l'utilisation des signatures numériques dans leurs relations entre eux et avec les tiers afin de renforcer l'acceptation et la confiance du public à l'égard des signatures numériques et de la communication électronique;
5. considère que le problème de la garantie de l'intégrité des informations peut être résolu du point de vue technique en même temps que celui de l'authenticité, de sorte qu'une intervention particulière de la Communauté n'est pas nécessaire à cet égard;
6. estime, en ce qui concerne le problème de la garantie de la confidentialité, que la priorité doit être accordée pour l'heure à la mise à disposition de toute personne participant à la communication électronique de techniques de chiffrement, mais qu'il y a lieu de tenir compte aussi des intérêts légitimes des autorités policières et judiciaires;
7. invite la Commission et les États membres à promouvoir le dialogue ainsi que des accords, au niveau international, à l'effet de rendre possible, grâce à des normes techniques communes et à la reconnaissance mutuelle, un espace économique virtuel couvrant l'ensemble de la planète;
8. estime que, eu égard au marché unique, les dispositions relatives aux biens à usage mixte devraient être modifiées à l'effet de supprimer le contrôle communautaire des produits de chiffrement de manière à assurer la libre circulation de ces produits;
9. invite les États membres à plaider, dans le cadre des discussions relatives à l'accord de Wassenaar et de la proposition de modification des dispositions relatives aux biens à usage mixte, pour que la liste des produits de chiffrement soumis à des restrictions d'exportation soit réduite au minimum et que, par conséquent, aucune nouvelle restriction ne soit mise en place;
10. souligne l'importance du dialogue international entre l'Union européenne et différents organismes internationaux tels que l'OCDE, les Nations unies, l'UIT, la CCI et l'OMC, afin d'éviter une situation en vertu de laquelle la réglementation constituerait une entrave au

commerce avec nos grands partenaires commerciaux, et souligne la nécessité de la réciprocité en ce qui concerne le traitement réservé à l'Union européenne par ses partenaires commerciaux;

11. estime que le développement du commerce électronique suppose un degré de confiance suffisant parmi les utilisateurs et qu'il y a lieu de fixer des normes en ce qui concerne la fiabilité juridique de l'identification, de la validité des contrats, de l'intégrité et de la communication, notamment;
12. souligne qu'il y a lieu de définir des règles générales qui, d'une part, assurent un renforcement de la confiance à l'égard du commerce électronique et, d'autre part, soient suffisamment souples et ouvertes pour faire face à de nouveaux développements techniques, par exemple dans le domaine de biométrie, une incitation au développement du commerce électronique, les normes et autres détails semblables pouvant être fixés par les entreprises;
13. est d'avis qu'il y a lieu d'oeuvrer en vue de la reconnaissance juridique des signatures numériques, la reconnaissance en tant que preuve en justice et la reconnaissance de l'équivalence avec le document écrit constituant deux points de départ importants;
14. souligne l'importance de la reconnaissance mutuelle des signatures numériques par les États membres ainsi que la nécessité de définir des normes minimales au niveau européen pour les signatures numériques, les États membres gardant la liberté de prévoir des normes plus rigoureuses à condition que ces normes complémentaires soient proportionnelles et que cela n'entrave pas les importations de biens et de services provenant d'autres États membres;
15. estime que le système de normes minimales permettrait aux États membres de susciter la confiance à l'égard de la qualité et de la fiabilité du régime de certificat, tout en leur laissant la liberté d'appliquer ou pas un système d'autorisation dans ce domaine;
16. souhaite, en tout état de cause, qu'il soit prévu dans la directive relative aux signatures numériques que la certification transfrontalière est possible; dans ce contexte, on pourrait envisager un organisme qui, à la demande de tiers d'un autre État membre, garantisse que la certification a été effectuée dans l'État membre concerné;
17. estime qu'il y a lieu de fixer des conditions communautaires pour la création et l'exploitation d'autorités de certification, par exemple une obligation d'enregistrement et d'indépendance par rapport au bénéficiaire du certificat; dans ce contexte, il serait opportun que, dans chaque État membre au moins une autorité de certification contrôle de manière objective, non discriminatoire et transparente le respect de ces normes, étant donné que cela renforcerait la confiance à l'égard du marché et serait bénéfique au climat d'investissement international;
18. constate que la rapidité de l'évolution technique qui s'opère dans le domaine du commerce électronique et, partant, la multitude des services nouveaux font qu'il n'y a pas de schéma uniforme pour la certification - vérification de l'identité, délivrance des certificats, annulation de ceux-ci, enregistrement du moment où le contrat électronique est conclu - au sein d'un ou plusieurs organismes, ce qui rend souhaitable, pour le moment, une certaine décantation;
19. demande instamment que soit établie une distinction claire entre services touchant à l'authentification et à l'intégrité, d'une part, et services relatifs à la confidentialité, d'autre part, et demande à la Commission d'élaborer sans retard une proposition de directive relative aux signatures numériques afin de promouvoir le commerce électronique, l'emploi et la

compétitivité de l'Union européenne dans ce domaine; invite en outre la Commission à suivre de près les nouvelles initiatives législatives prises dans ce domaine dans les États membres afin de faciliter le bon fonctionnement du marché intérieur;

20. estime que, sous l'angle du marché unique, il y a lieu de modifier le règlement relatif aux biens à usage mixte de manière à supprimer les contrôles intracommunautaires sur les produits de chiffrement afin que ces produits puissent circuler librement;
21. appelle les États membres à prendre, dans le cadre des discussions concernant l'accord de Wassenaar et la proposition – pratiquement prête – visant à modifier le règlement relatif aux biens à double usage, les dispositions nécessaires pour que la liste des produits de chiffrement soumis à restrictions à l'exportation soit réduite au strict minimum; de nouvelles restrictions ne doivent donc pas être instaurées;
22. souligne l'importance du dialogue international entre l'Union européenne et différentes organisations internationales telles que l'OCDE, les Nations unies, l'UIT, la CCI et l'OMC, étant donné qu'il y a lieu d'éviter que la réglementation n'entrave les échanges avec des partenaires commerciaux importants, et souligne la nécessité de la réciprocité en matière de traitement réservé à l'Union européenne par ses partenaires commerciaux;
23. estime que le cinquième programme-cadre de recherche et de développement de l'Union européenne devrait prévoir des crédits suffisants pour inciter les entreprises européennes à renforcer leurs efforts dans les domaines du chiffrement, de la normalisation et des produits interopérables aux normes américaines ou présentant une interface commune avec ceux-ci;
24. invite tous les secteurs de la société, notamment les entreprises européennes, à développer des normes communes dans ce domaine, non seulement au niveau national mais aussi au niveau international en veillant à ce que ces normes soient conformes aux meilleures pratiques et à l'état actuel de la technique;
25. considère que le commerce électronique peut devenir l'un des moteurs du développement de la société de l'information planétaire. Ce nouvel espace économique «virtuel», qui présente un grand potentiel de création d'emplois, est toutefois menacé par le manque de sécurité et de confiance sur les réseaux ouverts;
26. souligne que l'action de l'Union européenne est essentielle pour établir une réglementation commune facilitant la libre circulation des biens et des services et le commerce électronique sur Internet, en promouvant la sécurité des technologies cryptographiques et la reconnaissance de la signature numérique et du chiffrement entre les États membres. Une telle reconnaissance permettra de développer l'offre communautaire de services et la réglementation communautaire relative aux «autorités de certification» qui, par leur contrôle, contribueront notamment au respect des droits d'auteur, à la protection de la vie privée et à la création d'un cadre de confiance;
27. souscrit à la volonté de faire émerger un marché européen du chiffrement, qui pourrait présenter, malgré les controverses sur les usages illicites, un grand intérêt pour le développement du commerce électronique et pour garantir le droit fondamental à la vie privée et à la confidentialité des communications, garanti par les constitutions des États membres, l'article 12 de la

Déclaration universelle des droits de l'homme et l'article 8 de la Convention européenne des droits de l'homme;

28. rappelle que la communication électronique ne se limite pas au territoire de l'Union européenne, et que l'adoption d'un système communautaire harmonisé concernant la signature digitale et le chiffrement devra également permettre à la Communauté de prendre l'initiative dans les négociations et le dialogue avec d'autres instances internationales, telles que l'OCDE (Organisation pour la coopération et le développement économique) et l'OMC (Organisation mondiale du commerce);
29. soutient les programmes prévus par la Commission, notamment Infosec II, et les projets de recherche du cinquième programme-cadre (1998-2002) sur le commerce électronique, et notamment sur les techniques permettant d'améliorer la protection de la vie privée et des données personnelles. Il convient enfin d'inviter les institutions de l'Union européenne à utiliser la signature digitale et le chiffrement, afin de contribuer à diffuser et à améliorer la confiance dans ces nouvelles technologies;
30. charge son Président de transmettre la présente résolution à la Commission et au Conseil.

B. EXPOSÉ DES MOTIFS

1. Position du problème

La Commission considère que le commerce électronique est appelé à devenir un des moteurs du développement de la société de l'information planétaire.

Cela est assurément exact, mais on ne saurait méconnaître que non seulement les techniques de signatures numériques et de chiffrement présentent une importance pour le commerce mais que, en outre, elles prendront de plus en plus de place dans la vie du simple citoyen, notamment dans ses rapports avec les autorités publiques.

Tout comme le commerce traditionnel, le commerce électronique implique la conclusion de contrats. Ceux-ci sont conclus par échange de déclarations d'intérêt convergentes. Lesdites déclarations sont normalement émises sous forme écrite. Cela signifie, par exemple au regard du droit allemand, que le document qui comporte la déclaration doit être signé par l'auteur de la déclaration lui-même ou qu'il doit porter une signature certifiée (article 126, paragraphe 1 BGB). La signature doit être autographe. Une reproduction mécanique (timbre fac-similé), la transmission par télégramme ou télécopieur, etc. ne suffisent pas, à moins que la loi ne prévoie une dérogation.

Le commerce électronique passant par les réseaux dits ouverts, c'est-à-dire accessibles à tous, pose trois problèmes par rapport au commerce traditionnel et compte tenu des critères et exigences évoqués ci-dessus qui devraient être, pour l'essentiel, communs à tous les systèmes juridiques européens.

1.1. Authenticité

La signature exigée pour une déclaration d'intention écrite a pour objet d'assurer que la déclaration soit soumise au droit.

Dans le commerce électronique, la signature de la personne physique est remplacée par une signature numérique. Il s'agit d'une formule produite au moyen d'une clé privée. L'authentification de la formule suppose un procédé permettant au destinataire d'une information numérique de s'assurer de l'origine de ladite information (pour de plus amples détails, voir annexe I de la communication de la Commission).

La nécessité d'un cadre juridique a été reconnue dans tous les États membres de l'UE. La France s'est dotée d'une nouvelle loi relative aux télécommunications, l'Allemagne a adopté une loi sur les signatures numériques et l'Italie une loi sur l'usage des documents et des contrats électroniques. Au Royaume-Uni, aux Pays-Bas, en Belgique, au Danemark et en Suède, des lois sont en cours d'élaboration (communication de la Commission, page 19).

Il y a risque de fragmentation juridique, ce qui aurait de lourdes conséquences sur le fonctionnement du marché unique.

1.2. Intégrité

Outre l'authenticité d'une information dans le commerce électronique, il n'est pas garanti que le contenu d'une information ne puisse être modifié en cours de transmission par des tiers ou par inadvertance (intégrité). La solution technique réside de nouveau dans l'emploi d'une signature numérique qui ne concerne pas le chiffrement du texte lui-même, mais exclusivement celui de la signature qui accompagne le texte en clair et doit permettre au destinataire de vérifier s'il y a eu modification des données.

1.3. Confidentialité

La Commission considère que le commerce électronique et de nombreuses autres applications de la société de l'information ne se développeront et n'offriront leurs bénéfices économiques et sociaux que si la confidentialité peut être assurée de manière conviviale et à un bon rapport coût/efficacité (communication de la Commission, page 12). Il est évident que le consommateur qui utilise des services comme le télé-achat ou la télébanque doit avoir la certitude que ses données personnelles, par exemple son numéro de carte de crédit, demeurent secrètes. En cas de contact professionnel par le truchement de réseaux ouverts, les entreprises doivent pouvoir se protéger de l'espionnage (détail d'un projet, appel d'offres, résultats de recherches).

Cela dit, les autorités policières et judiciaires craignent que la diffusion du recours à la communication cryptée n'entrave la lutte contre la criminalité.

Le cryptage ne fait l'objet d'un contrôle public qu'en France, où l'utilisation de la cryptographie est soumise depuis 1990 à déclaration dans les cas simples et à autorisation dans les autres (communication de la Commission, page 14).

2. Solutions avancées par la Commission

2.1. Authenticité

Dans le domaine de la communication électronique, la signature numérique est couplée à l'emploi d'une sorte de sceau électronique apposé sur les données à transmettre et qui donne au destinataire la possibilité de vérifier l'origine des données ou, plus précisément, l'emploi d'une clé attribuée à un expéditeur déterminé. Cette vérification de l'authenticité n'établit toutefois pas nécessairement l'identité du détenteur de la clé. Le destinataire d'une information ne peut par exemple pas déterminer si l'expéditeur est réellement la personne qu'il prétend être. La possibilité existe par exemple d'utiliser une clé "publique" sous un autre nom. Une possibilité pour le destinataire de s'assurer de l'identité de l'expéditeur consiste à obtenir confirmation d'un tiers, une personne ou un organisme, auquel les deux parties font confiance. Dans le contexte des signatures numériques, ces organismes tiers sont généralement appelés autorités de certification (pour de plus amples détails, voir communication, pages 3-9).

La communication de la Commission n'apporte pas de formule claire pour résoudre ces problèmes nouveaux liés à l'authenticité.

Elle évoque, d'une part, le principe de reconnaissance mutuelle:

"Dans un cadre réellement international pour le commerce électronique, les certificats alloués par des AC étrangères doivent être reconnus mutuellement dans différents pays ... Les structures nationales pourraient être complétées par un mécanisme de coordination au niveau européen."

Par ailleurs est envisagée la possibilité d'une procédure de certification uniforme:

"D'autres possibilités pour assurer la confiance au niveau transfrontalier consisteraient en des services de certification européens harmonisés (y compris les procédures concernant l'allocation d'un tel certificat), de même que des critères et des procédures d'évaluation communes⁽¹⁾".

Enfin, la Commission donne l'impression de n'avoir pas beaucoup avancé dans les préparatifs d'une réglementation communautaire:

"La Commission évaluera la possibilité de procéder à l'harmonisation des différentes dispositions nationales afin de soutenir la reconnaissance mutuelle des signatures numériques au plan international⁽²⁾".

2.2. Intégrité

Comme il a déjà été indiqué, il est apparu que la meilleure solution technique consistait à prévoir deux clés pour les signatures numériques: une clé publique, qui est communiquée, et une clé privée, qui reste secrète. Afin de vérifier que la signature a bien été générée au moyen de la clé privée, on peut utiliser la clé publique correspondante. La clé publique de l'expéditeur permet au destinataire de vérifier aussi si les données ont été altérées. Le destinataire peut donc déterminer si la clé publique et la clé privée de l'expéditeur constituent une paire complémentaire et si les données ont été altérées lors de la transmission.

Cet exercice ne nécessite pas l'intervention d'une autorité de certification. La Commission n'évoque donc pas la nécessité d'une réglementation dans ce domaine.

2.3. Confidentialité

La Commission a transmis au Parlement le 22 septembre 1997 une proposition de directive relative à la protection juridique des données cryptées. La commission juridique examinera bientôt le projet de rapport de M. Anastassopoulos. Cette proposition concerne en premier lieu la protection des droits d'auteur et la préservation du secret professionnel, qui, à côté de la vie privée, rendent indispensable la possibilité de chiffrement dans les réseaux ouverts.

En ce qui concerne le droit correspondant du citoyen à la protection contre l'usage abusif de ces techniques de chiffrement (notamment espionnage, terrorisme et agissements criminels), la Commission se montre beaucoup plus réticente. Des dispositions qui entraveraient l'utilisation de produits et de services de chiffrement à l'intérieur du marché unique entraveraient par conséquent la circulation sûre et libre d'informations à caractère personnel et de biens et services connexes. Il

⁽¹⁾ Les deux citations sont extraites du point 2.4. de la communication.

⁽²⁾ Point 3 de la communication.

ne serait pas possible d'empêcher efficacement que les criminels se servent de procédés de chiffrement performants ou qu'ils contournent un dépôt de clé. Les avantages d'une réglementation en matière de lutte contre la criminalité ne sont donc pas faciles à évaluer et sont souvent présentés de manière schématique⁽¹⁾.

La Commission ne considère donc pas ce secteur comme une priorité d'action. Elle se limitera plutôt à vérifier si des réglementations nationales comme la loi française du 29 décembre 1990 sur la cryptographie "peuvent être totalement ou partiellement justifiées, en particulier au vu des dispositions du traité en matière de libre circulation et des dispositions de la directive communautaire sur la protection des données"⁽²⁾.

3. Évaluation

Parmi les trois problèmes évoqués, le premier, celui de l'authenticité dans les communications électroniques, est le premier qui pourrait et devrait être abordé par la Commission. Les questions à traiter pourraient ressortir par exemple de la loi allemande sur les signatures numériques du 22 juillet 1997. Il va toutefois sans dire que cette loi n'aborde pas la question de la classification des signatures numériques en droit civil.

La carence de la Commission dans ce domaine est d'autant plus incompréhensible qu'elle souligne à plusieurs reprises dans sa communication qu'un cadre communautaire est requis d'urgence et devrait être mis en place d'ici à l'an 2000⁽³⁾. Le problème de l'intégrité des données transmises est apparemment résolu dès lors qu'est appliqué d'une manière générale le système des deux clés complémentaires publique et privée. Il n'y aurait donc pas nécessité d'une action communautaire dans ce domaine.

Le problème de la confidentialité ou du chiffrement des données pourrait encore échauffer les esprits durant longtemps. La Commission mise à l'évidence sur la promotion d'un nouveau marché des techniques, des services et des produits et juge indispensable le développement de ce marché dans la perspective de la société de l'information.

⁽¹⁾ Communication de la Commission, pp. 17-18.

⁽²⁾ Communication de la Commission, p. 20.

⁽³⁾ Communication de la Commission, p. 18.

23 avril 1998

AVIS

(article 147 du règlement)

à l'intention de la commission juridique et des droits des citoyens

sur la communication de la Commission au Conseil, au Parlement européen, au Comité économique et social, 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" (COM(97)0503 - C4-0648/97) (rapport de M. Wolfgang Ullmann)

Commission économique, monétaire et de la politique industrielle

Rapporteur pour avis: M. W.G. van Velzen

PROCÉDURE

Au cours de sa réunion du 21 janvier 1998, la commission économique, monétaire et de la politique industrielle a nommé M. W.G. van Velzen rapporteur pour avis.

Au cours de ses réunions des 24 mars et 23 avril 1998, elle a examiné le projet d'avis.

Au cours de la dernière de ces réunions, elle a adopté les conclusions ci-après à l'unanimité.

Étaient présents au moment du vote les députés Karl von Wogau, président; Katiforis et Secchi, vice-présidents; W.G. van Velzen, rapporteur pour avis; Areitio Toledo, Argyros (suppléant M. de Brémond d'Ars), Arroni, Boogerd-Quaak (suppléant M. Gasòliba i Böhm), Camisón Asensio (suppléant M. Fourçans), Carlsson, Cassidy (suppléant M. Friedrich), Caudron, Christodoulou, Cox, Donnelly, Filippi (suppléant M. García-Margallo y Marfil), Funk (suppléant M. Konrad), Glante, Harrison, Herman, Hoppenstedt, Ilaskivi, Kestelijn-Sierens, Kuckelkorn, Langen, de Lassus (suppléant M. Castagnède), Lindqvist (suppléant Mme Larive), Lulling, Erika Mann (suppléant Mme Berès), Thomas Mann (suppléant M. Mather), Metten, Mezzaroma, Miller, Murphy, Paasilinna, Peijs, Pérez Royo, Peter (suppléant M. Billingham), Porto (suppléant M. Rübzig), Rapkay, de Rose, Skinner (suppléant Mme Read), Soltwedel-Schäfer, Tappin (suppléant M. Wibe), Thyssen, Torres Marques, Watson et Wolf (suppléant Mme Hautala).

1. Introduction

Les réseaux ouverts comme Internet sont de plus en plus utilisés pour la communication et pour le commerce électroniques. Cette évolution peut contribuer dans une large mesure au développement mondial de la société de l'information. En ce qui concerne l'Union européenne, le développement du commerce électronique offre des possibilités non négligeables de croissance économique et de création d'emploi. De plus, les consommateurs peuvent profiter sans cesse davantage de nouvelles formes de communication et de commerce électroniques. Le manque de sécurité qui va de pair avec le recours aux réseaux ouverts entrave toutefois une utilisation optimale des avantages du commerce et de la communication électroniques. Il est possible d'intercepter et de modifier des informations, de nier la validité d'un document ou de collecter de manière illicite des données personnelles. Les techniques de cryptage telles que les signatures numériques et le chiffrement peuvent apporter une contribution notable à l'amélioration de la sécurité et à la confiance dont jouissent les réseaux ouverts. Un certain nombre d'États membres ont annoncé leur intention de légiférer dans ce domaine ou l'ont déjà fait. Toutefois, des réglementations divergentes ne seraient pas favorables au bon fonctionnement du marché intérieur. C'est pourquoi la mise en place d'une politique commune de l'Union européenne en matière de signatures numériques et de chiffrement constitue une condition indispensable du succès du commerce électronique en Europe.

2. Signatures numériques

Les signatures numériques constituent actuellement une réponse reconnue au manque de sécurité qui caractérise l'emploi des réseaux ouverts. Cela n'exclut pas qu'à l'avenir le progrès technique apporte d'autres solutions. La réglementation doit donc être indépendante de la technique, ce qui signifie qu'elle doit pouvoir être adaptée avec souplesse en cas de nouvelles évolutions techniques. Simultanément, elle doit être suffisamment claire pour donner confiance aux utilisateurs: ceux-ci doivent avoir la certitude que les transactions sont effectivement effectuées, être sûrs de l'identité véritable de l'acheteur et du vendeur et avoir la certitude que la communication entre les deux parties s'effectue sans perturbations ni falsifications. Il s'agit là de conditions fondamentales.

Pour répondre à la question de savoir si l'expéditeur d'une information est effectivement celui qu'il prétend être, il faut généralement faire intervenir une autorité de certification capable de vérifier l'identité des personnes concernées. Cette autorité peut aussi tenir un registre des certificats délivrés, avec indication de leur date d'expiration. L'évolution rapide du marché est à l'origine de l'apparition de toutes sortes d'organismes jouant le rôle d'autorité de certification, et l'on ne saurait parler d'un schéma uniforme.

L'absence de réglementation communautaire peut constituer un obstacle à la confiance transfrontalière à l'égard des autorités de certification. La définition de normes communautaires en matière de certification revêt une grande importance du point de vue de la reconnaissance mutuelle des certificats relatifs aux signatures numériques. Il y aurait lieu de définir au niveau européen des normes minimales. Les États membres garderaient la liberté d'opter pour un système d'autorisation ou pour l'autodiscipline, à condition qu'il soit satisfait à ces normes minimales. Quiconque satisferait à ces normes pourrait fournir des biens et des services sur tout le territoire de l'Union. Il pourrait aussi s'avérer nécessaire de prévoir différentes catégories de certificat, de telle sorte que les niveaux de sécurité et de confiance soient identiques dans tous les États membres.

Eu égard au caractère passionné de la discussion relative aux règles d'accès aux clés de chiffrement, il importe d'établir une distinction claire entre services d'authentification et d'intégrité d'une part (signatures numériques) et services de confidentialité d'autre part (chiffrement).

3. Chiffrement

Le chiffrement de données est actuellement le principal moyen d'assurer la confidentialité des communications électroniques et des documents informatisés. L'accroissement rapide de la demande de produits de chiffrement dans le monde entier s'accompagne d'une expansion des possibilités offertes aux entreprises mais aussi en matière d'emploi en Europe. Dans ce domaine, les chances de cette dernière ne sont pas négligeables, à condition que soit créé un climat favorable. Il faut entendre par là une approche plus concentrée de la recherche dans ce domaine, le développement de produits européens interopérables et une meilleure normalisation. Les citoyens et les entreprises d'Europe peuvent prétendre à ce que leurs opérations financières s'effectuent dans les meilleures conditions de sécurité. À cet égard, l'Europe ne saurait admettre que son sort dépende de la question de savoir si les autorités américaines, pour des raisons difficiles à cerner, autorisent ou pas l'exportation des techniques de chiffrement.

Les services de recherche et de sécurité plaident en faveur de règles légales en matière d'accès aux clés de chiffrement, et ce par souci de sécurité nationale et pour assurer la lutte contre la criminalité et le terrorisme. Les inconvénients de la démarche résident dans une augmentation des possibilités d'aliénation, d'atteinte à la vie privée, dans le rapport coût/efficacité. Par ailleurs peut se poser la question de savoir si le dépôt de clés ne porte pas atteinte à la confiance de l'utilisateur à l'égard de la communication électronique. Une possibilité pourrait consister à rendre obligatoire l'accès à l'information cryptée dès lors que l'on dispose d'une demande dûment autorisée. Cela pourrait se réaliser en prévoyant que chacun soit tenu de déposer sa clé personnelle auprès d'un tiers de confiance ("Trusted Third Party"). Critères auxquels il y aurait lieu de satisfaire en cas de demande en ce sens: nécessité, efficacité et proportionnalité. Le problème est que le citoyen obéissant fournira vraisemblablement une copie de sa clé, ce que les criminels ne feront assurément pas. On peut donc s'attendre à ce que la mesure ne produise pas de résultats uniformes. De plus, des mesures restrictives constitueraient une entrave notable au développement des biens et services sur le marché du chiffrement. Des dispositions en matière d'accès sont donc à déconseiller fortement. Au demeurant, la France est le seul État membre de l'UE à avoir réglementé le chiffrement.

4. Dialogue international

L'article 19, paragraphe 1, du règlement relatif aux biens à usage mixte, qui prévoit des contrôles nationaux, prévoit aussi une révision de la nécessité de ces contrôles dans un délai de trois ans à compter de la date d'entrée en vigueur. Ce délai est venu à expiration à la fin de l'année 1997. Dans l'optique du marché intérieur, il est à recommander de modifier ce règlement de manière à supprimer (par étapes) les contrôles intracommunautaires frappant les produits de chiffrement. Une restriction devrait pouvoir être prévue en ce qui concerne le chiffrement de pointe, c'est-à-dire le chiffrement à usage militaire ou diplomatique. En tout état de cause, il importe que le chiffrement commercial puisse circuler librement dans l'intérêt du commerce électronique.

Eu égard au caractère transfrontalier de la communication électronique, le dialogue international entre différents organismes internationaux tels que OCDE, Nations unies, OMPI, UIT, OIT, OMC et CCI revêt une grande importance. Il convient aussi d'éviter que les normes minimales

européennes n'entravent les échanges avec nos grands partenaires commerciaux, par exemple les États-Unis et le Japon.

5. Conclusions

La commission économique, monétaire et de la politique industrielle invite la commission juridique et des droits des citoyens, compétente au fond, à incorporer dans son rapport les conclusions ci-après:

1. estime que le développement du commerce électronique suppose un degré de confiance suffisant parmi les utilisateurs et qu'il y a lieu de fixer des normes en ce qui concerne la fiabilité juridique de l'identification, de la validité des contrats, de l'intégrité et de la communication, notamment;
2. souligne qu'il y a lieu de définir des règles générales qui, d'une part, assurent un renforcement de la confiance à l'égard du commerce électronique et, d'autre part, soient suffisamment souples et ouvertes pour faire face à de nouveaux développements techniques, par exemple dans le domaine de biométrie, une incitation au développement du commerce électronique, les normes et autres détails semblables pouvant être fixés par les entreprises;
3. est d'avis qu'il y a lieu d'oeuvrer en vue de la reconnaissance juridique des signatures numériques, la reconnaissance en tant que preuve en justice et la reconnaissance de l'équivalence avec le document écrit constituant deux points de départ importants;
4. souligne l'importance de la reconnaissance mutuelle des signatures numériques par les États membres ainsi que la nécessité de définir des normes minimales au niveau européen pour les signatures numériques, les États membres gardant la liberté de prévoir des normes plus rigoureuses à condition que ces normes complémentaires soient proportionnelles et que cela n'entrave pas les importations de biens et de services provenant d'autres États membres;
5. estime que le système de normes minimales permettrait aux États membres de susciter la confiance à l'égard de la qualité et de la fiabilité du régime de certificat, tout en leur laissant la liberté d'appliquer ou pas un système d'autorisation dans ce domaine;
6. souhaite, en tout état de cause, qu'il soit prévu dans la directive relative aux signatures numériques que la certification transfrontalière est possible; dans ce contexte, on pourrait envisager un organisme qui, à la demande de tiers d'un autre État membre, garantisse que la certification a été effectuée dans l'État membre concerné;
7. estime qu'il y a lieu de fixer des conditions communautaires pour la création et l'exploitation d'autorités de certification, par exemple une obligation d'enregistrement et d'indépendance par rapport au bénéficiaire du certificat; dans ce contexte, il serait opportun que, dans chaque État membre au moins une autorité de certification contrôle de manière objective, non discriminatoire et transparente le respect de ces normes, étant donné que cela renforcerait la confiance à l'égard du marché et serait bénéfique au climat d'investissement international;
8. constate que la rapidité de l'évolution technique qui s'opère dans le domaine du commerce électronique et, partant, la multitude des services nouveaux font qu'il n'y a pas de schéma uniforme pour la certification - vérification de l'identité, délivrance des certificats, annulation

de ceux-ci, enregistrement du moment où le contrat électronique est conclu - au sein d'un ou plusieurs organismes, ce qui rend souhaitable, pour le moment, une certaine décantation;

9. constate qu'une réglementation de la responsabilité est indispensable pour assurer la confiance dans l'utilisation des produits cryptés, mais estime que, pour le moment, il n'y a pas lieu de prévoir des dispositions supplémentaires à cet égard au niveau européen, étant donné que la réglementation existante est suffisante, ce qui n'exclut pas que les États membres puissent mettre en place des dispositions complémentaires liées à la portée des contrats, dès lors que cela n'entrave pas les importations de biens et de services d'autres États membres, et invite la Commission à suivre de près l'évolution dans ce domaine et, au besoin, à proposer les mesures appropriées au niveau européen;
10. demande instamment que soit établie une distinction claire entre services touchant à l'authentification et à l'intégrité, d'une part, et services relatifs à la confidentialité, d'autre part, et demande à la Commission d'élaborer sans retard une proposition de directive relative aux signatures numériques afin de promouvoir le commerce électronique, l'emploi et la compétitivité de l'Union européenne dans ce domaine; invite en outre la Commission à suivre de près les nouvelles initiatives législatives prises dans ce domaine dans les États membres afin de faciliter le bon fonctionnement du marché intérieur;
11. souligne expressément que nulle disposition en matière d'accès aux clés ne doit être instaurée, étant donné que la mesure est disproportionnée par rapport au résultat escompté, eu égard, notamment, à l'accroissement des risques de vol des clés, à l'atteinte à la vie privée et au rapport coût/efficacité;
12. estime que, sous l'angle du marché unique, il y a lieu de modifier le règlement relatif aux biens à usage mixte de manière à supprimer les contrôles intracommunautaires sur les produits de chiffrement afin que ces produits puissent circuler librement;
13. appelle les États membres à prendre, dans le cadre des discussions concernant l'accord de Wassenaar et la proposition – pratiquement prête – visant à modifier le règlement relatif aux biens à double usage, les dispositions nécessaires pour que la liste des produits de chiffrement soumis à restrictions à l'exportation soit réduite au strict minimum; de nouvelles restrictions ne doivent donc pas être instaurées;
14. souligne l'importance du dialogue international entre l'Union européenne et différentes organisations internationales telles que l'OCDE, les Nations unies, l'UIT, la CCI et l'OMC, étant donné qu'il y a lieu d'éviter que la réglementation n'entrave les échanges avec des partenaires commerciaux importants, et souligne la nécessité de la réciprocité en matière de traitement réservé à l'Union européenne par ses partenaires commerciaux;
15. estime que le cinquième programme-cadre de recherche et de développement de l'Union européenne devrait prévoir des crédits suffisants pour inciter les entreprises européennes à renforcer leurs efforts dans les domaines du chiffrement, de la normalisation et des produits interopérables aux normes américaines ou présentant une interface commune avec ceux-ci;

16. invite tous les secteurs de la société, notamment les entreprises européennes, à développer des normes communes dans ce domaine, non seulement au niveau national mais aussi au niveau international en veillant à ce que ces normes soient conformes aux meilleures pratiques et à l'état actuel de la technique.

AVIS
(Article 147 du règlement)

à l'intention de la commission juridique et des droits des citoyens

sur la communication de la Commission «Assurer la sécurité et la confiance dans la communication électronique. Vers un cadre européen pour les signatures numériques et le chiffrement» (COM(97)0503 - C4-0648/97) (rapport Ullmann)

Commission de la culture, de la jeunesse, de l'éducation et des médias

Lettre du président de la commission à M. Willy De Clercq, président de la commission juridique et des droits des citoyens

Bruxelles, le 22 avril 1998

Monsieur le Président,

Au cours de sa réunion du 22 avril 1998, la commission de la culture, de la jeunesse, de l'éducation et des médias a examiné le sujet mentionné sous rubrique.

Au cours de cette dernière réunion, elle a adopté les conclusions suivantes⁽¹⁾:

1. La commission de la culture, de la jeunesse, de l'éducation et des médias considère que le commerce électronique peut devenir l'un des moteurs du développement de la société de l'information planétaire. Ce nouvel espace économique «virtuel», qui présente un grand potentiel de création d'emplois, est toutefois menacé par le manque de sécurité et de confiance sur les réseaux ouverts.
2. L'action de l'Union européenne est essentielle pour établir une réglementation commune facilitant la libre circulation des biens et des services et le commerce électronique sur Internet, en promouvant la sécurité des technologies cryptographiques et la reconnaissance de la signature numérique et du chiffrement entre les États membres. Une telle reconnaissance permettra de développer l'offre communautaire de services et la réglementation communautaire relative aux

⁽¹⁾ Ont participé au vote les députés Pex, président; Hawlicek et Ahlqvist, vice-présidents; Añoberos Trias de Bes, Banotti, Daskalaki (suppléant M. Boniperti), De Esteban Martin (suppléant M^{me} Heinisch), Elchlepp (suppléant M. De Coene), Fontaine, Guinebertière, Günther (suppléant M. Escudero), Kerr, Kuhne, Mouskouri, Pack, Rynnänen, Sanz Fernandez, Todini (suppléant M^{me} Poisson).

«autorités de certification» qui, par leur contrôle, contribueront notamment au respect des droits d'auteur, à la protection de la vie privée et à la création d'un cadre de confiance.

3. La commission de la culture s'inquiète des éventuelles utilisations illicites du chiffrement, qui pourraient profiter de la confidentialité pour mener à bien des activités criminelles et terroristes, et souligne la nécessité de distinguer le chiffrement de la signature digitale, qui permet de prévenir les fraudes en authentifiant et en garantissant l'intégrité et de protéger les transactions des consommateurs.
4. Elle souscrit à la volonté de faire émerger un marché européen du chiffrement, qui pourrait présenter, malgré les controverses sur les usages illicites, un grand intérêt pour le développement du commerce électronique et pour garantir le droit fondamental à la vie privée et à la confidentialité des communications, garanti par les constitutions des États membres, l'article 12 de la Déclaration universelle des droits de l'homme et l'article 8 de la Convention européenne des droits de l'homme.
5. La communication électronique ne se limite pas au territoire de l'Union européenne, et l'adoption d'un système communautaire harmonisé concernant la signature digitale et le chiffrement devra également permettre à la Communauté de prendre l'initiative dans les négociations et le dialogue avec d'autres instances internationales, telles que l'OCDE (Organisation pour la coopération et le développement économique) et l'OMC (Organisation mondiale du commerce).
6. La commission de la culture soutient les programmes prévus par la Commission, notamment Infosec II, et les projets de recherche du cinquième programme-cadre (1998-2002) sur le commerce électronique, et notamment sur les techniques permettant d'améliorer la protection de la vie privée et des données personnelles. Il convient enfin d'inviter les institutions de l'Union européenne à utiliser la signature digitale et le chiffrement, afin de contribuer à diffuser et à améliorer la confiance dans ces nouvelles technologies.

Veillez agréer, Monsieur le Président, l'expression de mes sentiments distingués.

(s.) Peter Pex