Sécurité des communications électroniques: services cryptés, signatures numériques, chiffrement

1997/2235(COS) - 06/10/1994

LEGISLATION COMMUNAUTAIRE PRECEDENTE: Aucune législation n'a encore été adoptée au niveau communautaire en ce qui concerne le cryptage des télécommunications. Le Conseil a adopté le 31.04.1992 une décision en matière de sécurité des systèmes d'information[(1) Décision 92/242/CEE, JO L 123, 8.05.1992, p. 19.] sur proposition de la Commission[(2) Proposition COM/90/314, JO C 277, 5.11.1990, p. 18.]. Il s'agissait de l'adoption d'un plan d'action de 24 mois et de la création d'un groupe de hauts fonctionnaires sur la sécurité de l'information(SOGIS)composé de deux représentants de chaque État membre et de la Commission, chargés de conseiller cette dernière. POSITION PRECEDENTE DU PE: Lors de l'examen de la proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel[(3) COM/90/314 final, JO C 277, 5.11.90, p. 3; avis du PE A3-0010/92, sur le rapport de M. Hoon Geoffrey W., JO C 94, 13.04.92, p. 76, 77, 173, 198; proposition modifiée COM/92/422 final, JO C 311, 27.11.92, p. 30 et COM/93/570.], le Parlement n'a pas amendé l'article 18 précisant que le responsable du traitement doit prendre les mesures techniques et d'organisation appropriées nécessaires à la protection contre la communication et toute autre forme de traitement non-autorisé de données personnelles. SITUATION DANS LES ETATS MEMBRES: L'intérêt des États est de pouvoir contrôler étroitement et rapidement les télécommunications dans le cadre de leur politique de lutte contre la criminalité et l'espionnage, en procédant à des écoutes téléphoniques et à des interceptions d'échanges de données. Cet intérêt se heurte à celui des individus qui veulent sauvegarder une sphère de liberté et de vie privée, que les services de police et de contre-espionnage pourraient avoir tendance à restreindre au nom de la sécurité publique. L'intérêt des groupes commerciaux est similaire, quant à lui, dans le domaine du secret des affaires. Mais en outre, il s'agit pour eux de défendre la possibilité de créer, produire et commercialiser des procédés de codage sans contrainte administrative, et sans être limité par la normalisation d'un procédé qui handicaperait les progrès en la matière. La France est actuellement le seul pays de la Communauté à posséder une loi sur les procédés de cryptologie (loi du 29.12.1990). Autrefois soumis au sévère régime des matériels de guerre, les procédés sont aujourd'hui soumis: * à une procédure de déclaration lorsqu'ils ont pour objet l'authentification d'une communication, ou la vérification de l'intégrité d'un message transmis, * à une procédure plus contraignante de licence obligatoire lorsqu'ils ne rentrent pas dans la première catégorie, la demande d'autorisation étant déposée avec la clé du codage auprès du Service de la sécurité des informations rattaché au Premier Ministre. Des procédures simplifiées peuvent être adoptées. Dans les autres États membres, les procédés de cryptage sont de libre usage et de libre commerce, sauf bien entendu si l'utilisateur est l'objet d'une obligation de secret d'Etat ou de la défense nationale. Mais plusieurs États sont préoccupés par la multiplication des télécommunications codées, aussi bien dans le réseau GSM utilisé par les radiotéléphones, que dans les échanges de données informatiques. Les Pays-Bas illustrent cette attitude. Une loi sur les délits informatiques est entrée en vigueur le 1er mars 1993, qui donne une base légale spécifique aux interceptions d'échanges des données, aux perquisitions de systèmes informatiques et à l'obtention de données décryptées ou des clés de décodage. D'autre part, un projet de loi de mai 1994 entendait soumettre les utilisateurs de procédés de cryptage à une procédure de licence et de dépôt des clés des codes devant une agence spéciale tenue par une obligation de secret. L'agence devait fournir ces clés aux services de police et de sécurité qui seraient munis d'un mandat adéquat. A la suite d'une fuite dans la presse, de nombreuses protestations conduisirent le gouvernement à abandonner son projet. Il convient de signaler l'importance de la politique américaine dans le domaine du cryptage. La NSA a menée en la matière une politique délibérée pour entraver l'exportation des procédés de codage sophistiqués, et pour promouvoir dans les communications avec les administrations un procédé standard nommé "Clipper chip", dont elle aurait possédé une clé universelle. La généralisation de l'emploi de ce procédé lui aurait en outre

permis de pouvoir considérer comme suspect tout codage par un moyen différent, utilisant par exemple le logiciel "Pretty Good Privacy" (PGP) qui a été largement communiqué sur Internet par son auteur pour lutter contre la politique du gouvernement américain. Les efforts de la NSA, et ceux du vice-président Al Gore, ont cependant échoué face aux réticences des entreprises américaines et des associations privées.