Security in electronic communication: digital signatures and encryption

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

PREVIOUS COMMUNITY LEGISLATION: No legislation has yet been adopted at Community level concerning the encryption of telecommunications. On 31 April 1992 the Council adopted a Commission proposal[(2) Proposal COM(90)0314, OJ C 277, 5.11.1990, p.18] for a decision in the field of information security[(3) Decision 92/242/EEC, OJ L 123, 8.05.1992, p.19]. It involved the adoption of a 24-month action plan and the establishment of a Senior Officials Group on Information Security (SOGIS), comprising two representatives from each Member State and the Commission, with a mandate to advise the Commission. PREVIOUS POSITION OF THE EP: When it considered the proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data[(4) COM (90)0314, OJ C 277, 5.11.1990, p. 3; opinion of the EP A3-0010/92 on the basis of a report by Mr Geoffrey W. Hoon, OJ C 94, 13.04.1992, p. 76,77, 173, 198; amended proposal COM(92)0422 final, OJ C 311, 27.11.1992, p. 30 and COM(93)0570.], Parliament did not amend Article 18 stipulating that the controller of a file must take appropriate technical and organizational measures to protect personal data from communication or any other unauthorized use. SITUATION IN THE MEMBER STATES: The Member States need to be able to monitor telecommunications closely and rapidly, as part of their policy for combating crime and espionage, by means of telephone tapping and intercepting exchanges of data. This clashes with the interests of individuals who wish to preserve a sphere of freedom and private life which the police and counter-espionage services could tend to restrict in the name of public security. Commercial groups have a similar interest in the area of commercial secrecy. However, they will also be concerned to retain the possibility of developing, producing and marketing encoding systems free of administrative constraints and without being restricted by the standardization of a system which would hold up progress in this field. France is currently the only country in the Community with a law on encryption systems (Law of 29 December 1990). Previously subject to the strict rules governing military equipment, these systems are now subject to: * a declaration procedure where they are designed to authenticate a communication or verify that a message transmitted is intact, * a more binding licensing procedure where they do not fall within the above category, the application for authorization being submitted with the encoding key to the information security service attached to the Prime Minister's office. Simplified procedures may be adopted. In the other Member States, encryption systems are freely used and freely sold, unless of course the user is bound by the rules governing state secrets or national defence. However, many countries are concerned at the proliferation of encoded telecommunications, both in the GSM network used by radiotelephones and in the exchange of electronic data. The Netherlands is an example of this attitude. A law on computer crime came into force on 1 March 1993, which provides a specific legal basis for the interception of the exchange of data, the searching of computer systems and the obtaining of decrypted data or decoding keys. In addition, a draft law of May 1994 sought to make users of encryption systems subject to a procedure for licensing and registration of code keys with a special agency bound to secrecy. The agency was to pass the keys on to the police and security services which would be given appropriate powers. Following a leak to the press, the many protests which ensued forced the government to abandon its plans. American policy is important in this field. The NSA has pursued a deliberate policy of preventing the export of sophisticated encoding systems, and promoting in communications with the authorities a standard system known as the 'Clipper chip', to which it was thought to have a universal key. The widespread use of this system would also have allowed it to consider as suspect any other form of encoding, using for example the 'Pretty Good Privacy' (PGP) software which has been transmitted widely on the Internet by its author to fight against the policy of the American government. However, faced by the reluctance of American business and private associations the efforts of the NSA and Vice-President Al Gore have failed.