Echelon interception system

2001/2098(INI) - 03/07/2001

The Temporary Committee on the Echelon Interception System adopted the own-initiative report by Gerhard SCHMID (PES, D) winding up the work it had carried out over the previous year. The first task of the committee, as laid down in its mandate, was to verify the existence of this interception system. While there was no formal proof, the committee said that in view of the evidence and the many statements which tallied with each other, including some from American sources, the existence of a global system for intercepting communications, operating with the participation of the USA, the UK, Canada, Australia and New Zealand under the UK-USA Agreement, was no longer in doubt. The same was true of the use to which Echelon was put, namely "to intercept private and commercial communications, and not military communications". While the capabilities of the system were not nearly as extensive as some sections of the media had assumed, it was worrying that many senior Community figures who gave evidence to the committee claimed to be unaware of the system. The committee's second task was to verify whether the system was compatible with Community law. The report distinguished between legitimate intelligence-gathering and the use of such a system to spy on business communications. In the latter case, any Member State participating in the system would be violating EU law. While the committee did not unearth any evidence that the global interception system was used to distort business competition, the report said that, according to information obtained in the USA, 5% of intelligence gathered through non-open sources was used for economic intelligence and that this intelligence surveillance could enable US industry to earn up to 7 billion dollars in terms of contracts. It pointed out that since sensitive data were mostly kept inside individual firms, other methods of espionage were generally used. Only if sensitive data were transmitted externally could communications surveillance be effective. In this connection the report called on the Member States and the US Government to start an open US-EU dialogue on economic intelligence-gathering. The mandate also covered the issue of privacy and the possibility for the committee to propose political or legislative initiatives. In this connection the committee called on the Member States to provide all European citizens with the same legal guarantees concerning the protection of privacy. The Member States were also urged to ensure that their legislation on the operations of their intelligence services was consistent with the European Human Rights Convention and the case-law of the European Court of Human Rights. In addition, they should endow themselves with binding instruments which afforded effective protection against all forms of illegal interception of their communications. The report argued that all the national parliaments should have a body responsible for scrutinising the activities of the intelligence services. In addition the Member States should pool their communications interception resources with a view to enhancing the effectiveness of the ESDP in the areas of intelligence-gathering and the fight against terrorism "subject to monitoring by the European Parliament, the Council and the Commission". In addition Germany and the UK were asked to make the authorisation of any further communications interception operations on their territory by US intelligence services conditional on certain requirements. The committee stressed the importance of fostering awareness of security problems among the public and companies so that they understood the potential risks and the need to protect themselves against the danger of having their communications intercepted. It made a number of practical proposals, including support for the development of European encryption software. The Commission was asked to take a range of measures: to have a security analysis carried out, to update its encryption system, to ensure that data was protected in its own data processing systems and to improve the protection of secrecy in relation to documents not accessible to the public. Lastly the Commission was requested to put forward a proposal to establish, in close cooperation with industry and the Member States, a European-wide and coordinated network of advisory centres to deal with issues relating to the security of information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance. Companies themselves were urged to cooperate more closely with counter-espionage services and particularly to inform them of any suspected attacks from outside.