SPEECH/01/368

Mr Erkki Liikanen

Member of the European Commission, responsible for Enterprise and the Information Society

European Parliament motion for a resolution on the Echelon interception system

EP motion for a resolution on the Echelon interception system

Strasbourg, 5 September 2001

President and Honourable Members,

I would like to congratulate Mr. Coelho, chairman, and the honourable members of the Parliament who participated in the work of the Temporary Committee on Echelon, and especially the rapporteur Mr. Schmid, with the comprehensive and well written report on the Echelon interception system.

Context

The Commission has been following the parliamentary work over the past year with great interest. The issue touches upon complex technological and political considerations. The report presents a large number of references to the existence of a global interception system. These build up a body of evidence.

The Commission already stated on 30 March last year: “It is the very nature of intelligence activities that those who are not involved in these activities are not able to confirm, nor deny their existence”. Even though the Commission is not involved in ‘intelligence gathering’ activities, we do not put in question the findings of the European Parliament.

The present report of the ECHELON temporary committee is based on careful and thorough work.

The European Union is founded on the respect for human rights and fundamental freedoms (art 6 of TEU and EU Charter of fundamental rights). As the guardian of the Treaty, the European Commission attaches the utmost importance to the respect of these principles.

The abuse of large-scale communications intelligence is something that can make an individual living in a democratic society feel uneasy. Privacy is a fundamental right. Any derogation from this right has to be specifically provided for by law, necessary for objectives of general interest, proportionate, and subject to adequate checks and guarantees against any form of misuse.

The Commission is determined to look at the practical implications of the EU Charter of fundamental rights, where, in particular, the protection of communications and personal data will be further enhanced. The Commission has already stated that it considers it would be preferable for the Charter to be integrated into the Treaties for the sake of visibility and legal certainty.

At the same time, the Community has to act within the scope of the competencies conferred upon it by the Treaty.

Compatibility with EU law

The findings of the Committee concerning the compatibility of a system of the ‘Echelon type’ with EU law distinguish between two scenarios:

- whether such a system is used purely for intelligence purposes,
- or the system is abused for the purpose of gathering competitive intelligence.

The Commission shares the opinion that operations envisaged in the first scenario in the interest of State security fall under the scope of Title V of the Treaty on European Union which sets out the framework for the establishment of a Common Foreign and Security Policy.

This lays down no provisions on intelligence activities. Member States remain responsible for the conduct and supervision of intelligence operations unless the Council decides otherwise. The EU treaty does not empower the Commission to exercise its prerogatives as guardian of the Treaty in this field.

Maintaining an interception system for the purpose of gathering intelligence in the context of a Member State's defence or national security is outside the scope of the directives in force on data protection.

As to the second scenario, gathering of competitive intelligence does not come within the scope of a common foreign and security policy. It is not an activity that would be allowed under the guise of the pursuit of a Common Foreign and Security Policy.

In so far as Community law is concerned, such activity could fall within the scope of the data protection directives. This is the case if data gathered by Echelon type systems is collected or subsequently passed on to commercial undertakings for purposes unrelated to the prevention of criminal offences and unrelated to State security matters.

Technological developments in electronic communications

We are all aware that electronic communications play and increasingly important role in everyday life. Well functioning electronic communications infrastructures are crucial for our economies.

Europe wants to become the most competitive and dynamic knowledge-based economy in the world. A pre-condition to achieve this is the need to build trust in electronic communications. This concerns both our citizens and our businesses.

The development in technologies can bring protection against surveillance. It is a comforting finding that the use of fibre optic cables instead of satellites for trans-continental communications has decreased the possibilities for large-scale routine interception.

The argument that the rise of the commercial Internet has diminished significantly the possibilities for interception is convincing. Today, the majority of Internet communications by cable no longer leave the European continent.

Commission policy to improve information security

The Commission has taken important steps over the past years in order to develop a policy to improve the security of electronic communications.

The availability and free circulation of encryption products and technologies in the European Union has now been ensured with the dual use regulation in place since September 2000. The support through the Community's Research Framework Programme, in particular the Information Society Technologies program, has improved the conditions to develop top of the range European encryption products in order to enable EU citizens, companies and governments to protect their communications.

However, this is not sufficient to guarantee a wide spread use of encryption. Especially citizens and small businesses are not always aware of the potential threats. We need to inform them about the possibilities of encryption.

In June this year, the Commission adopted a Communication on Network and Information Security. The purpose is to tackle this awareness problem and to further develop a European approach on security related issues. I am very glad to notice that the conclusions of the report we are discussing here today are very much in line with the approach adopted by the Commission.

The Honourable Members know that there is already a legal framework in place at EU level addressing data protection and obligations for operators. There is also an emerging policy on cybercrime. Network and Information security is now coming in as a third element, to complete the picture.

Although the Communication is not meant to contain a fully-fledged 'action plan' we have already identified some broad action lines where progress needs to be made.

I will highlight some of them:

- to raise awareness public information and education campaigns should be launched and best practices should be promoted;
- a European warning and information system is needed to strengthen the activities of Computer Emergency Response Teams (CERTs) or similar entities and improve the co-ordination amongst them; I have noted the Parliament's support for this idea;
- examine how to best organise at European level pro-active and co-ordinated measures to develop forward looking responses to existing and emerging security threats (e. g. an Information Security Observatory);
- concerning the legal framework we will set up an inventory of national measures, which have been taken in accordance with relevant Community law.

I would also like to mention that further action is needed to support the development of technology, streamlined standardisation and certification work, the introduction of security in government use and better international co-operation.

As a next step it is our intention to develop a roadmap before the end of this year containing concrete actions with firm deadlines in order to start putting a European Information Security policy in place.

Commission's own information systems

The Commission is constantly improving the protection of its own information systems in terms of availability, integrity and confidentiality, especially in view of the changing nature of the various existing and potential threats.

The entry point to the Commission network is constantly monitored and actively tested. Similar efforts are conducted through projects for secure video conferencing, secure telephone systems and encryption of databases. Furthermore security audits of Commission information systems are conducted on a regular basis.

A new **Information Systems Security Policy** has been drafted and is currently being prepared for discussion within Commission services. In addition the Commission is reviewing its overall security policy as a result of internal reorganisation activities and policy developments (e.g. Common Foreign and Security Policy, Justice and Home Affairs).

The new internal Commission security provisions, will follow the model of the Council Security regulation adopted earlier this year, and will be based on the following principles:

- proportionality of security measures in relation to existing risks,
- shared responsibility and accountability of staff, management and security experts,

- integration of all elements into a coherent security strategy (e.g. personnel, information and physical security)
- close co-operation between European and national security organisations.

The Commission intends to allocate additional resources to the security domain. However, scarce technical and human resources, especially in the field of information security specialists, do hamper the full deployment of security policies. This concern is common to most public administrations, including the European Institutions. I welcome the support in the report to allocate more resources for the tasks to be undertaken in this field.

I sincerely hope that the budgetary authorities will follow this position.

Conclusion

President, the trust of European citizens and businesses in electronic communications and the well functioning of information infrastructures has become crucial for our economies.

Let me reiterate once more in this perspective that the Commission attaches the utmost importance to the respect of Human Rights and the respect of Rules of Law.

Thank you.