27. Urges the Member States to ratify the Montreal Convention as soon as possible to improve the protection of passengers in the event of accident and to enable the updating of Council Regulation (EC) No 2027/97; in this regard, stresses the importance of clear and easily accessible information to air passengers on applicable liability limits, including the relevant time limits for issuing complaints, which should be automatically provided by airline companies whilst booking;

28. Considers that accessibility of air travel must be improved for all passengers, including for disabled passengers, children and the elderly;

29. Welcomes the efforts made by airlines to implement staff training activities in the field of assistance to passengers in general, and those with reduced mobility in particular;

30. Calls on the Commission to bring forward legislative proposals to prohibit any European Union airline or airport from charging an extra fee to persons with reduced mobility for being assisted onto or off any aeroplane in the European Union;

Health aspects

31. Considers that health should be given a higher profile and that the air passengers and crew should be sufficiently informed about the health aspects of air travel;

32. Recommends that the airlines give pre-take-off health briefing on long-haul flights comparable to the safety briefing already required and that such information be available to passengers on their tickets, in particular concerning preventative action;

33. Calls on the Commission as a matter of urgency to allocate monies from the EU research budget to carry out an independent evaluation of the possible public health risks for air passengers who travel on long-haul flights, including carrying out a comprehensive study into the whole issue of deep vein thrombosis; calls on the Commission to carry out this independent research in consultation with EU airline companies and with EU consumer groups;

34. Calls on European Union airlines to inform passengers of the percentage degree seat pitch available to passengers travelling in economy class;

*

* *

35. Instructs its President to forward this resolution to the Council and the Commission.

---

21. Echelon

A5-0264/2001

European Parliament resolution on the existence of a global system for the interception of private and commercial communications (Echelon interception system) (2001/2098(INI))

The European Parliament,

— having regard to its decision of 5 July 2000 to set up a Temporary Committee on the Echelon Interception System and the mandate issued to the Temporary Committee [1],

— having regard to the EC Treaty, one objective of which is the establishment of a common market with a high level of competitiveness,

[1] OJ C 121, 24.4.2001, p. 131.

Wednesday 5 September 2001

— having regard to Articles 11 and 12 of the Treaty on European Union, which impose on the Member States a binding requirement to enhance and develop their mutual political solidarity,

— having regard to the Treaty on European Union, in particular Article 6(2) thereof, which lays down the requirement that the EU must respect fundamental rights, and Title V thereof, which sets out provisions governing the common foreign and security policy,

— having regard to Article 12 of the Universal Declaration of Human Rights,

— having regard to the Charter of Fundamental Rights of the EU, Article 7 of which lays down the right to respect for private and family life and explicitly enshrines the right to respect for communications, and Article 8 of which protects personal data,

— having regard to having regard to the European Convention on Human Rights (ECHR), in particular Article 8 thereof, which governs the protection of private life and the confidentiality of correspondence, and the many other international conventions which provide for the protection of privacy,

— having regard to the work carried out by the Temporary Committee on the Echelon Interception System, which held a large number of hearings and meetings with experts of all kinds, and in particular with senior representatives of the public and private sectors in the sphere of telecommunications and data protection, with employees of intelligence and information services, with journalists, with lawyers with expert knowledge of this area, with members of the national parliaments of the Member States, etc.,

— having regard to Rule 150(2) of its Rules of Procedure,

— having regard to the report of the Temporary Committee on the Echelon Interception System (A5-0264/2001),

The existence of a global system for intercepting private and commercial communications (the Echelon interception system)

A. whereas the existence of a global system for intercepting communications, operating by means of cooperation proportionate to their capabilities among the US, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt; whereas it seems likely, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that its name is in fact Echelon, although this is a relatively minor detail,

B. whereas there can now be no doubt that the purpose of the system is to intercept, at the very least, private and commercial communications, and not military communications, although the analysis carried out in the report has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed,

C. whereas, therefore, it is surprising, not to say worrying, that many senior Community figures, including European Commissioners, who gave evidence to the Temporary Committee claimed to be unaware of this phenomenon,

The limits of the interception system

D. whereas the surveillance system depends, in particular, upon worldwide interception of satellite communications, although in areas characterised by a high volume of communications only a very small proportion of those communications are transmitted by satellite; whereas this means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals, something which — as the investigations carried out in connection with the report have shown — is possible only to a limited extent; whereas the numbers of personnel required for the final analysis of intercepted communications imposes further restrictions; whereas, therefore, the UKUSA states have access to only a very limited proportion of cable and radio communications and can analyse an even more limited proportion of those communications, and whereas, further, however extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice,

The possible existence of other interception systems

E. whereas the interception of communications is a method of spying commonly employed by intelligence services, so that other states might also operate similar systems, provided that they have the required funds and the right locations; whereas France is the only EU Member State which is — thanks to its overseas territories — geographically and technically capable of operating autonomously a global interception system and also possesses the technical and organisational infrastructure to do so; whereas there is also ample evidence that Russia is likely to operate such a system,

Compatibility with EU law

F. whereas, as regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios: if a system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union (CFSP), although at present that title lays down no provisions on the subject, so that no criteria are available; if, on the other hand, the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyal cooperation and with the concept of a common market based on free competition, so that a Member State participating in such a system violates EC law,

G. having regard to the statements made by the Council at the plenary sitting of 30 March 2000 to the effect that 'the Council cannot accept the creation or existence of a telecommunications interception system which does not respect the laws of the Member States and which violates the fundamental principles aimed at protecting human dignity',

Compatibility with the fundamental right to respect for private life (Article 8 of the ECHR)

H. whereas any interception of communications represents serious interference with an individual's exercise of the right to privacy; whereas Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference; whereas interference must be proportionate, so that competing interests need to be weighed up and, under the terms of the case law of the European Court of Human Rights, it is not enough that the interference should merely be useful or desirable,

I. whereas an intelligence system which intercepted communications permanently and at random would be in violation of the principle of proportionality and would not be compatible with the ECHR; whereas it would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable, or if the interference was not proportionate; whereas most of the rules governing the activities of US intelligence services abroad are classified, so that compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and foreseeability laid down by the European Court of Human Rights probably occur,

J. whereas the Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance,

K. whereas, in addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus; whereas the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, so that there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinising the secret services,

Wednesday 5 September 2001

Are EU citizens adequately protected against intelligence services?

L. whereas the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and whereas in some cases parliamentary monitoring bodies do not even exist, so that the degree of protection can hardly be said to be adequate; whereas it is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinising the activities of the intelligence services; whereas even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it is only the former which affect their own citizens; whereas it would be an encouragement for proportionate interference practices, if intelligence services were obliged to notify a citizen whose communications have been intercepted of this fact afterwards, for example five years after the interception took place,

M. whereas, in view of their size, satellite receiving stations cannot be built on the territory of a state without its consent,

N. whereas, in the event of cooperation between intelligence services under the CFSP or in the areas of justice and home affairs, the institutions must introduce adequate measures to protect European citizens,

Industrial espionage

O. whereas part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc., and whereas, for these reasons, the firms concerned are often subject to surveillance,

P. whereas the US intelligence services do not merely investigate general economic facts but also intercept detailed communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery; whereas detailed interception poses the risk that information may be used for the purpose of competitive intelligence-gathering rather than combating corruption, even though the US and the United Kingdom state that they do not do so; whereas, however, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled,

Q. whereas an agreement on combating the bribery of officials, under which bribery is criminalised at international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications,

R. whereas the situation becomes intolerable when intelligence services allow themselves to be used for the purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country, and whereas it is frequently maintained that the global interception system has been used in this way, although no such case has been substantiated,

S. whereas, during the visit by the delegation from the Temporary Committee to the US, authoritative sources confirmed the US Congress Brown Report, indicating that 5 % of intelligence gathered via non-open sources is used as economic intelligence; whereas it was estimated by the same sources that this intelligence surveillance could enable US industry to earn up to USD 7 billion in contracts,

T. whereas sensitive commercial data are mostly kept inside individual firms, so that competitive intelligence-gathering in particular involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else, more and more commonly, by hacking

into internal computer networks; whereas only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence-gathering; whereas this applies systematically in the following three cases:

- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;
- in the case of videoconferencing within multinationals using VSAT or cable;
- if vital contracts are being negotiated on the spot (e.g. for the building of plants, telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the firm's head office,

U. whereas risk and security awareness in small and medium-sized firms is often inadequate and the dangers of economic espionage and the interception of communications are not recognised,

V. whereas security awareness is not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations) and action is therefore necessary,

Possible self-protection measures

W. whereas firms can only make themselves secure by safeguarding their entire working environment and protecting all communications channels which are used to send sensitive information; whereas sufficiently secure encryption systems exist at affordable prices on the European market; whereas private individuals should also be urged to encrypt e-mails; whereas an unencrypted e-mail message is like a letter without an envelope; whereas relatively user-friendly systems exist on the Internet which are even made available for private use free of charge,

Cooperation among intelligence services within the EU

X. whereas the EU has reached agreement on the coordination of intelligence-gathering by intelligence services as part of the development of its own security and defence policy, although cooperation with other partners in these areas will continue,

Y. whereas in December 1999 in Helsinki the European Council decided to develop more effective European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP; whereas the European Council decided furthermore that, in order to achieve this goal, by the year 2003 the Union should be able to deploy rapidly units of about 50 000-60 000 troops which should be self-sustaining, including the necessary command, control and intelligence capabilities; whereas the first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee,

Z. whereas cooperation among intelligence services within the EU seems essential on the grounds that, firstly, a common security policy which did not involve the secret services would not make sense, and, secondly, it would have numerous professional, financial and political advantages; whereas it would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR; whereas the European Parliament would of course have to exercise appropriate monitoring,

AA. whereas the European Parliament is in the process of implementing European Parliament and Council Regulation (EC) No 1049/2001 of 30 May 2001 on public access to European Parliament, Council and Commission documents [1] by amending the provisions of its Rules of Procedure as regards access to sensitive documents,

[1] OJ L 145, 31.5.2001, p. 43.

Wednesday 5 September 2001

Conclusion and amendment of international agreements on the protection of citizens and firms

1. States, on the basis of the information obtained by the Temporary Committee, that the existence of a global system for intercepting communications, operating with the participation of the United States, the United Kingdom, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt;

2. Calls on the Secretary-General of the Council of Europe to submit to the Ministerial Committee a proposal to protect private life, as guaranteed in Article 8 of the ECHR, brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the European Court of Human Rights nor reduce the flexibility which is vital if future developments are to be taken into account;

3. Calls on the Member States — whose laws governing the interception capabilities of the secret services contain provisions on the protection of privacy which are discriminatory — to provide all European citizens with the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence;

4. Calls on the Member States of the European Union to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens' rights in order to scrutinise the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of the report of the European Parliament's temporary committee, and in particular Section 8.3.4.; emphasises the need to draw up joint standards which are better suited to the requirements of protecting the fundamental rights of EU citizens and more stringent than those guaranteed by Article 8 of the ECHR;

5. Calls on the Member States to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act at the next Intergovernmental Conference in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy;

6. Calls on the member countries of the Council of Europe to adopt an additional protocol which enables the European Communities to accede to the ECHR or to consider other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities;

7. Urges the EU institutions in the meantime to apply the fundamental rights enshrined in the ECHR and its protocols and in the Charter within the scope of their respective powers and activities;

8. Calls on the UN Secretary-General to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations;

9. Regards it as essential that an agreement should be negotiated and signed between the European Union and the United States stipulating that each of the two parties should observe, vis-à-vis the other, the provisions governing the protection of the privacy of citizens and the confidentiality of business communications applicable to its own citizens and firms;

10. Calls on the US to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the Covenant by the US can be submitted to the Human Rights Committee set up under the Covenant; calls on the relevant American NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), to exert pressure on the US Administration to that end;

National legislative measures to protect citizens and firms

11. Urges the Member States to review and if necessary to adapt their own legislation on the operations of the intelligence services to ensure that it is consistent with fundamental rights as laid down in the ECHR and with the case law of the European Court of Human Rights;

12. Calls on the Member States to endow themselves with binding instruments which afford natural and legal persons effective protection against all forms of illegal interception of their communications;

13. Calls on the Member States to aspire to a common level of protection against intelligence operations and, to that end, to draw up a Code of Conduct (as referred to in paragraph 4) based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services;

14. Calls on the Member States to negotiate with the US a Code of Conduct similar to that of the EU;

15. Calls on those Member States which have not yet done so to guarantee appropriate parliamentary and legal supervision of their secret services;

16. Urges the Council and the Member States to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level; proposes that the European Parliament should play an important role in this monitoring and control system;

17. Calls on the Member States to 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, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission;

18. Calls on the Member States to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions;

Specific legal measures to combat industrial espionage

19. Calls on the Member States to consider to what extent industrial espionage and the payment of bribes as a way of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void; calls on the United States, Australia, New Zealand and Canada to join this initiative;

20. Calls on the Member States to undertake to incorporate in the EC Treaty a clause prohibiting industrial espionage and not to engage in industrial espionage against one another, either directly or with the assistance of a foreign power which might carry out operations on their territory, nor to allow a foreign power to conduct espionage operations from the soil of an EU Member State, thereby complying with the letter and spirit of the EC Treaty;

21. Calls on the Member States to undertake by means of a clear and binding instrument not to engage in industrial espionage, thereby signifying their compliance with the letter and spirit of the EC Treaty; calls on the Member States to transpose this binding principle into their national legislation on intelligence services;

22. Calls on the Member States and the US Administration to start an open US-EU dialogue on economic intelligence-gathering;

Wednesday 5 September 2001

Measures concerning the implementation of the law and the monitoring of that implementation

23. Calls on the national parliaments which have no parliamentary monitoring body responsible for scrutinising the activities of the intelligence services to set up such a body;

24. Calls on the monitoring bodies responsible for scrutinising the activities of the secret services, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals;

25. Calls on the Member States to make sure that their intelligence systems are not misused for the purposes of gathering competitive intelligence, an act at odds with the Member States' duty of loyal cooperation and with the concept of a common market based on free competition;

26. Calls on Germany and the United Kingdom to make the authorisation of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorised or even merely tolerated on their territory respect human rights;

Measures to encourage self-protection by citizens and firms

27. Calls on the Commission and the Member States to inform their citizens and firms about the possibility that their international communications may, under certain circumstances, be intercepted; insists that this information should be accompanied by practical assistance in designing and implementing comprehensive protection measures, including the security of information technology;

28. Calls on the Commission, the Council and the Member States to develop and implement an effective and active policy for security in the information society; insists that as part of this policy specific attention should be given to increasing the awareness of all users of modern communication systems of the need to protect confidential information; furthermore, insists on the establishment of a Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies;

29. Urges the Commission and Member States to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software;

30. Calls on the Commission and Member States to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes;

31. Calls on the Commission to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the 'least reliable' category;

32. Calls on the European institutions and the public administrations of the Member States systematically to encrypt e-mails, so that ultimately encryption becomes the norm;

33. Calls on the Community institutions and the public administrations of the Member States to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses;

34. Calls for particular attention to be paid to the position of the applicant countries; urges that they should be given support, if their lack of technological independence prevents them from implementing the requisite protective measures;

Other measures

35. Calls on firms to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency;

36. Calls on the Commission to have a security analysis carried out which will show what needs to be protected, and to have a protection strategy drawn up;

37. Calls on the Commission to update its encryption system in line with the latest developments, given that modernisation is urgently needed, and calls on the budgetary authorities (the Council together with Parliament) to provide the necessary funding;

38. Proposes that its competent committee draw up an own-initiative report on security and the protection of secrecy in the European institutions;

39. Calls on the Commission to ensure that data is protected in its own data-processing systems and to step up the protection of secrecy in relation to documents not accessible to the public;

40. Calls on the Commission and the Member States to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Programme;

41. Urges states which have been placed at a disadvantage by distortions of competition resulting from state aid or the economic misuse of espionage to inform the authorities and monitoring bodies of the state from which the activities were undertaken in order to put a stop to the distorting activities;

42. Calls on the Commission to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centres — in particular in those Member States where such centres do not yet exist — to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance;

43. Takes the view that an international congress on the protection of privacy against telecommunications surveillance should be held in order to provide NGOs from Europe, the US and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action;

*

* *

44. Instructs its President to forward this resolution to the Council, the Commission, the Secretary-General and Parliamentary Assembly of the Council of Europe and the governments and parliaments of the Member States and applicant countries, the United States, Australia, New Zealand and Canada.