Bundesrat Drucksache **801/01**

28.09.01

Unterrichtung
durch das
Europäische Parlament

Entschließung des Europäischen Parlaments zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon)

Zugeleitet mit Schreiben des Generalsekretärs des Europäischen Parlaments - 121259 - vom 25. September 2001. Das Europäische Parlament hat die Entschließung in der Sitzung am 5. September 2001 angenommen.

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 1320, 53003 Bonn
Telefon: 0228/3820840, Telefax: 0228/3820844
ISSN 0720-2946

Entschließung des Europäischen Parlaments zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI))

Das Europäische Parlament,

– unter Hinweis auf seinen Beschluss vom 5. Juli 2000, einen nichtständigen Ausschuss über das Abhörsystem Echelon einzusetzen, und dessen Mandat[15],

– unter Hinweis auf den EG-Vertrag, der auf die Errichtung eines Gemeinsamen Marktes mit einem hohen Grad an Wettbewerbsfähigkeit abzielt,

– unter Hinweis auf Artikel 11 und 12 des EU-Vertrags, die die Mitgliedstaaten verpflichten, ihre gegenseitige politische Solidarität zu stärken und weiterzuentwickeln,

– unter Hinweis auf den EU-Vertrag, insbesondere dessen Artikel 6 Absatz 2, der die Verpflichtung der Europäischen Union zur Achtung der Grundrechte festschreibt, und auf Titel V, der Bestimmungen für eine Gemeinsame Außen- und Sicherheitspolitik (GASP) trifft,

– unter Hinweis auf Artikel 12 der Allgemeinen Menschenrechtserklärung,

– unter Hinweis auf die Charta der Grundrechte der Europäischen Union, deren Artikel 7 die Achtung des Privat- und Familienlebens schützt und ausdrücklich das Recht auf Achtung der Kommunikation vorsieht, sowie auf Artikel 8, der den Schutz personenbezogener Daten festlegt,

– unter Hinweis auf die Europäische Menschenrechtskonvention (EMRK), insbesondere ihren Artikel 8, der die Privatsphäre und die Vertraulichkeit des Briefverkehrs schützt, sowie die zahlreichen anderen internationalen Übereinkommen, die den Schutz der Privatsphäre vorsehen,

– unter Hinweis auf die vom Nichtständigen Ausschuss über das Abhörsystem Echelon durchgeführten Arbeiten, der zahlreiche Anhörungen und Sitzungen mit Sachverständigen verschiedenster Fachrichtungen abgehalten hat, insbesondere mit Verantwortlichen des öffentlichen und privaten Sektors im Bereich der Telekommunikation, des Datenschutzes, Mitarbeitern der Nachrichtendienste, Journalisten, auf dieses Gebiet spezialisierten Anwälten, Abgeordneten der nationalen Parlamente der Mitgliedstaaten usw.,

– unter Hinweis auf Artikel 150 Absatz 2 seiner Geschäftsordnung,

[15] ABl. C 121 vom 24. 4. 2001, S. 131.

– in Kenntnis des Berichts des nichtständigen Ausschusses über das Abhörsystem Echelon A5-0264/2001),

zur Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon)

A. in der Erwägung, dass an der Existenz eines weltweit arbeitenden Kommunikationsabhörsystems, das durch anteiliges Zusammenwirken der USA, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands im Rahmen des UKUSA-Abkommens funktioniert, nicht mehr gezweifelt werden kann; ferner in der Erwägung, dass es aufgrund der vorliegenden Indizien und dem übereinstimmenden Tenor von Erklärungen aus sehr unterschiedlichen Kreisen von Einzelpersonen und Organisationen – einschließlich amerikanischer Quellen – angenommen werden kann, dass sein Name in der Tat „Echelon" ist, was allerdings ein relativ unwichtiges Detail ist,

B. in der Erkenntnis, dass nunmehr kein Zweifel mehr daran bestehen kann, dass das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient, obgleich die im Bericht vorgenommene Analyse gezeigt hat, dass die technischen Kapazitäten dieses Systems wahrscheinlich bei Weitem nicht so umfangreich sind, wie von den Medien teilweise angenommen,

C. in der Erwägung, dass es deshalb erstaunlich, wenn nicht gar beunruhigend ist, dass zahlreiche Verantwortliche der Gemeinschaft, einschließlich Mitglieder der Kommission, die vom Nichtständigen Ausschuss angehört wurden, erklärt haben, dass sie keine Kenntnis von diesem Phänomen hätten,

zu den Grenzen des Abhörsystems

D. in der Erwägung, dass das Überwachungssystem insbesondere auf dem globalen Abhören von Satellitenkommunikation aufbaut, dass Kommunikation aber in Gebieten mit hoher Kommunikationsdichte nur zu einem sehr geringen Teil über Satelliten vermittelt wird; dass somit der überwiegende Teil der Kommunikation nicht durch Bodenstationen abgehört werden kann, sondern nur durch Anzapfen von Kabeln und Abfangen von Funk, was – wie die im Bericht vorgenommenen Untersuchungen gezeigt haben – nur in eng gesteckten Grenzen möglich ist; dass der Personalaufwand für die letztendliche Auswertung von abgefangener Kommunikation weitere Beschränkungen bedingt; dass die UKUSA-Staaten deshalb nur Zugriff auf einen sehr beschränkten Teil der kabel- und funkgebundenen Kommunikation haben und einen noch geringeren Teil der Kommunikation auswerten können, und ferner auch unter Hinweis darauf, dass, so umfangreich die verfügbaren Mittel und Kapazitäten zum Abhören von Kommunikationen auch sein mögen, ihre äußerst große Zahl in der Praxis eine erschöpfende und gründliche Kontrolle aller Kommunikationen unmöglich macht,

zur möglichen Existenz anderer Abhörsysteme

E. in der Erwägung, dass das Abhören von Kommunikation ein unter Nachrichtendiensten übliches Spionagemittel ist und ein solches System auch von anderen Staaten betrieben werden könnte, sofern sie über die entsprechenden finanziellen Mittel und die geographischen Voraussetzungen verfügen; in der Erwägung, dass Frankreich der einzige

Mitgliedstaat der Europäischen Union ist, der – aufgrund seiner überseeischen Gebiete – geographisch und technisch in der Lage ist, ein globales Abhörsystem autonom zu betreiben und der auch die technische und organisatorische Infrastruktur dafür besitzt; unter Hinweis darauf, dass es viele Anzeichen dafür gibt, dass Russland wahrscheinlich ein solches System betreibt,

zur Vereinbarkeit mit EU-Recht

F. in der Erwägung, dass betreffend die Frage der Vereinbarkeit eines Systems des Typs Echelon mit EU-Recht zwei Fälle zu unterscheiden sind: wird das System nur zu nachrichtendienstlichen Zwecken verwendet, so ergibt sich kein Widerspruch zu EU-Recht, da Tätigkeiten im Dienste der Staatssicherheit vom EGV nicht erfasst sind, sondern unter Titel V des EU-Vertrags (GASP) fallen würden, es derzeit dort aber noch keine einschlägigen Regelungen gibt und es somit an Berührungspunkten fehlt; wird das System hingegen zur Konkurrenzspionage missbraucht, so steht das System im Widerspruch zur Pflicht der Mitgliedstaaten zu loyaler Zusammenarbeit und zum Konzept eines gemeinsamen Marktes mit freiem Wettbewerb, so dass ein Mitgliedstaat, der sich daran beteiligt, EG-Recht verletzt,

G. unter Hinweis auf die Erklärungen der Ratstagung vom 30. März 2000, wonach der Rat "die Einrichtung oder Existenz eines Systems zur Überwachung des Fernmeldeverkehrs, das die Rechtsnormen der Mitgliedstaaten nicht achtet und die Grundprinzipien verletzt, die dem Schutz der Menschenwürde dienen, nicht hinnehmen kann",

zur Vereinbarkeit mit dem Grundrecht auf Privatsphäre (Artikel 8 EMRK)

H. in der Erwägung, dass jedes Abhören von Kommunikation einen tief greifenden Eingriff in die Privatsphäre des Einzelnen darstellt; dass Artikel 8 EMRK, der die Privatsphäre schützt, Eingriffe nur zur Gewährleistung der nationalen Sicherheit zulässt, sofern die Regelungen im innerstaatlichen Recht niedergelegt und allgemein zugänglich sind und festlegen, unter welchen Umständen und Bedingungen die Staatsgewalt sie vornehmen darf; dass Eingriffe darüber hinaus verhältnismäßig sein müssen, daher eine Interessenabwägung vorgenommen werden muss und nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) ein reines „Nützlich- oder Wünschenswertsein" nicht genügt,

I. in der Erwägung, dass ein nachrichtendienstliches System, das wahllos und dauerhaft jedwede Kommunikation abfangen würde, einen Verstoß gegen das Verhältnismäßigkeitsprinzip darstellen würde und mit der EMRK nicht vereinbar wäre; dass in gleicher Weise ein Verstoß gegen die EMRK vorläge, wenn die Regelung, nach der Kommunikationsüberwachung erfolgt, keine Rechtsgrundlage hat, wenn diese nicht allgemein zugänglich ist oder wenn sie so formuliert ist, dass ihre Konsequenzen für den Einzelnen nicht vorhersehbar sind, oder wenn der Eingriff nicht verhältnismäßig ist; dass die Regelungen, nach denen amerikanische Nachrichtendienste im Ausland tätig werden, großteils klassifiziert sind, die Wahrung des Verhältnismäßigkeitsprinzips somit zumindest fraglich ist, und ein Verstoß gegen die vom EGMR aufgestellten Prinzipien der Zugänglichkeit des Rechts und der Voraussehbarkeit seiner Wirkung wohl vorliegt,

J. in der Erwägung, dass sich die Mitgliedstaaten ihrer aus der EMRK erwachsenden Verpflichtungen nicht dadurch entziehen können, dass sie die Nachrichtendienste anderer

Staaten auf ihrem Territorium tätig werden lassen, die weniger strengen Bestimmungen unterliegen, da sonst das Legalitätsprinzip mit seinen beiden Komponenten der Zugänglichkeit und Voraussehbarkeit seiner Wirkung beraubt und die Rechtsprechung des EGMR in ihrem Inhalt ausgehöhlt würde,

K. in der Erwägung, dass die Grundrechtskonformität gesetzlich legitimierter Tätigkeit von Nachrichtendiensten zudem verlangt, dass ausreichende Kontrollsysteme vorhanden sind, um einen Ausgleich zur Gefahr zu schaffen, die das geheime Agieren eines Teiles der Verwaltung mit sich bringt; dass der EGMR ausdrücklich die Bedeutung eines effizienten Kontrollsystems im Bereich nachrichtendienstlicher Tätigkeit hervorhob und es deshalb bedenklich erscheint, dass einige Mitgliedstaaten über keine eigenen parlamentarischen Kontrollorgane für Geheimdienste verfügen,

zur Frage, ob EU-Bürger ausreichend vor Nachrichtendiensten geschützt sind

L. in der Erwägung, dass der Schutz der EU-Bürger von der Rechtslage in den einzelnen Mitgliedstaaten abhängt, diese aber sehr unterschiedlich gestaltet sind, teilweise sogar gar keine parlamentarischen Kontrollorgane bestehen und deshalb kaum von einem ausreichenden Schutz gesprochen werden kann; dass die europäischen Bürger ein fundamentales Interesse daran haben, dass ihre nationalen Parlamente mit einem formell strukturierten speziellen Kontrollausschuss ausgestattet sind, der die Aktivitäten der Nachrichtendienste überwacht und kontrolliert; dass selbst dort, wo es Kontrollorgane gibt, für diese der Anreiz groß ist, sich mehr um die Tätigkeit von Inlandsnachrichtendiensten als von Auslandsnachrichtendiensten zu kümmern, da in der Regel nur im ersten Fall die eigenen Bürger betroffen sind; dass es einen Anreiz für eine verhältnismäßige Abhörpraxis darstellen würde, wenn die Nachrichtendienste verpflichtet wären, einen Bürger, dessen Kommunikation abgehört worden ist, im Nachhinein über diese Tatsache zu unterrichten, beispielsweise fünf Jahre, nachdem der Eingriff erfolgt ist,

M. in der Erwägung, dass die Empfangssatelliten wegen ihrer Größe nicht ohne Zustimmung des betreffenden Landes auf dessen Hoheitsgebiet errichtet werden können,

N. in der Erwägung, dass im Falle einer Zusammenarbeit der Nachrichtendienste im Rahmen der GASP und der JIA (Justiz und Innere Angelegenheiten) die Institutionen gefordert sind, ausreichende Schutzbestimmungen zugunsten der europäischen Bürger zu schaffen,

zur Wirtschaftsspionage

O. in der Erwägung, dass es Bestandteil des Aufgabengebiets von Auslandsnachrichtendiensten ist, sich für wirtschaftliche Daten wie Branchenentwicklungen, Entwicklung von Rohstoffmärkten, Einhaltung von Wirtschaftsembargos, Einhaltung der Lieferregeln für Dual-use-Güter etc. zu interessieren, und dass aus diesen Gründen einschlägige Unternehmen oftmals überwacht werden,

P. in der Erwägung, dass die Nachrichtendienste der USA nicht nur allgemeine wirtschaftliche Sachverhalte aufklären, sondern Kommunikation von Unternehmen gerade bei Auftragsvergabe auch im Detail abhören und dies mit der Bekämpfung von Bestechungsversuchen begründen; dass bei detailliertem Abhören das Risiko besteht, dass die Informationen nicht zur Bekämpfung der Bestechung, sondern zur Konkurrenzspionage verwendet werden, auch wenn die USA und das Vereinigte Königreich erklären, dass sie

das nicht tun; dass aber die Rolle des Advocacy Centers des US-Handelsministeriums nach wie vor nicht völlig klar ist, und ein mit ihm vereinbartes Gespräch, das der Klärung dienen sollte, abgesagt wurde,

Q. in der Erwägung, dass im Rahmen der OECD 1997 ein Abkommen zur Bekämpfung der Bestechung von Beamten angenommen wurde, welches die internationale Strafbarkeit von Bestechung vorsieht, und deshalb auch unter diesem Aspekt Bestechung in einzelnen Fällen das Abhören von Kommunikation nicht rechtfertigen kann,

R. in der Erwägung, dass es jedenfalls nicht tolerierbar ist, wenn sich Nachrichtendienste für Konkurrenzspionage instrumentalisieren lassen, indem sie ausländische Unternehmen ausspionieren, um inländischen einen Wettbewerbsvorteil zu verschaffen, dass es allerdings keinen belegten Fall dafür gibt, dass das globale Abhörsystem dafür eingesetzt wurde, auch wenn dies vielfach behauptet wurde,

S. in der Erwägung, dass zuverlässige Quellen während des Besuchs der Delegation des Nichtständigen Ausschusses über das Abhörsystem Echelon in den USA den Brown-Bericht des US-Kongresses bestätigt haben, wonach 5 % der nachrichtendienstlichen Informationen, die durch nicht offen zugängliche Quellen gewonnen wurden, zum Sammeln von Wirtschaftsdaten verwendet werden; dass die Sammlung derartiger Daten Schätzungen derselben Quellen zufolge die US-Industrie in die Lage versetzen könnte, bei Verträgen Einnahmen in Höhe von bis zu 7 Milliarden Dollar zu erzielen,

T. im Hinblick darauf, dass sich sensible Unternehmensdaten vielfach in den Unternehmen selbst befinden, so dass Konkurrenzspionage vor allem dadurch erfolgt, dass versucht wird, über Mitarbeiter oder eingeschleuste Personen Informationen zu bekommen und zunehmend in die internen Computernetzwerke einzudringen; dass nur wenn sensible Daten über Leitungen oder via Funk (Satellit) nach außen gelangen, ein Kommunikationsüberwachungssystem zur Konkurrenzspionage eingesetzt werden kann und dies systematisch nur in folgenden drei Fällen zutrifft:

- bei Unternehmen, die in drei Zeitzonen arbeiten, so dass die Zwischenergebnisse von Europa nach Amerika und weiter nach Asien gesandt werden;

- im Falle von Videokonferenzen in multinationalen Konzernen, die über V-Sat oder Kabel laufen;

- wenn wichtige Aufträge vor Ort verhandelt werden (wie im Anlagenbau, Aufbau von Telekommunikationsinfrastruktur, Neuerrichtung von Transportsystemen, etc.) und von dort aus Rücksprachen mit der Firmenzentrale gehalten werden müssen,

U. in der Erwägung, dass Risiko- und Sicherheitsbewusstsein bei kleinen und mittleren Unternehmen oft unzureichend sind und die Gefahren der Wirtschaftsspionage und des Abhörens von Kommunikation nicht erkannt werden,

V. in der Erwägung, dass bei den Europäischen Institutionen (mit Ausnahme der Europäischen Zentralbank, der Generaldirektion Auswärtige Beziehungen des Rates sowie der Generaldirektion Außenbeziehungen der Kommission) das Sicherheitsbewusstsein nicht immer sehr ausgeprägt ist und deshalb Handlungsbedarf besteht,

zu den Möglichkeiten, sich selbst zu schützen

W. in der Erwägung, dass Sicherheit für Unternehmen nur dann erzielt werden kann, wenn das gesamte Arbeitsumfeld abgesichert sowie alle Kommunikationswege geschützt sind, auf denen sensible Informationen übermittelt werden; dass es ausreichend sichere Verschlüsselungssysteme zu erschwinglichen Preisen auf dem europäischen Markt gibt; dass auch Privaten dringend zur Verschlüsselung von E-Mails geraten werden muss; dass eine unverschlüsselte Mail gleich einem Brief ohne Umschlag ist; dass sich im Internet relativ benutzerfreundliche Systeme finden, die sogar für den Privatgebrauch unentgeltlich zur Verfügung gestellt werden,

zur Zusammenarbeit der Nachrichtendienste innerhalb der Europäischen Union

X. in der Erwägung, dass sich die Europäische Union darauf verständigt hat, nachrichtendienstliche Informationssammlung im Rahmen der Entwicklung einer eigenen Sicherheits- und Verteidigungspolitik zu koordinieren, dabei aber die Zusammenarbeit mit anderen Partnern in diesen Bereichen fortzusetzen,

Y. in der Erwägung, dass der Europäische Rat im Dezember 1999 in Helsinki beschlossen hat, wirksamere europäische militärische Strukturen zu entwickeln, um der gesamten Palette der Petersberg-Aufgaben zur Unterstützung der GASP gerecht werden zu können; dass der Europäische Rat weiterhin beschlossen hat, dass die Union, um dieses Ziel zu erreichen, bis zum Jahr 2003 in der Lage sein soll, rasch Streitkräfte mit einer Stärke von 50 000 bis 60 000 Personen aufzustellen, die militärisch autonom sein sollten und über die erforderlichen Fähigkeiten in Bezug auf Streitkräfteführung und strategische Aufklärung sowie über die entsprechenden nachrichtendienstlichen Kapazitäten verfügen; dass die ersten Schritte hin zum Aufbau derartiger nachrichtendienstlicher Kapazitäten bereits im Rahmen der WEU sowie des ständigen Politischen und Sicherheitspolitischen Komitees unternommen wurden,

Z. in der Erwägung, dass eine Zusammenarbeit der Nachrichtendienste innerhalb der Europäischen Union auch unabdingbar erscheint, da einerseits eine Gemeinsame Sicherheitspolitik ohne Einbeziehung der Geheimdienste sinnwidrig wäre, andererseits damit zahlreiche Vorteile in professioneller, finanzieller und politischer Hinsicht verbunden wären; dass es auch eher der Idee eines gleichberechtigten Partners der USA entsprechen würde und sämtliche Mitgliedstaaten in ein System einbinden könnte, das in voller Konformität zur EMRK erstellt wird; dass eine entsprechende Kontrolle der Zusammenarbeit durch das Europäische Parlament dann natürlich gesichert sein muss,

AA. in der Erwägung, dass es im Begriff ist, die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission[16] im Wege der Anpassung seiner Geschäftsordnung betreffend den Zugriff auf sensible Dokumente umzusetzen,

---

[16] ABl. L 145 vom 31.5.2001, S. 43.

zu Abschluss und Änderung internationaler Verträge zum Schutz der Bürger und Unternehmen

1. betont die Tatsache, dass es auf der Grundlage der durch den Nichtständigen Ausschuss eingeholten Informationen keinen Zweifel mehr daran gibt, dass ein globales Abhörsystem existiert, das unter Beteiligung der Vereinigten Staaten, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands im Rahmen des UKUSA-Abkommens betrieben wird;

2. fordert den Generalsekretär des Europarats auf, dem Ministerkomitee einen Vorschlag zur Anpassung des in Artikel 8 EMRK garantierten Schutzes der Privatsphäre an die modernen Kommunikationsmethoden und Abhörmöglichkeiten in einem Zusatzprotokoll oder gemeinsam mit der Regelung des Datenschutzes im Rahmen einer Revision der Datenschutzkonvention zu unterbreiten, unter der Voraussetzung, dass dadurch weder eine Minderung des durch den Gerichtshof entwickelten Rechtsschutzniveaus noch eine Minderung der für die Anpassung an weitere Entwicklungen notwendigen Flexibilität bewirkt wird;

3. fordert die Mitgliedstaaten – deren Gesetze über die Überwachungsbefugnisse der Geheimdienste derartige Diskriminierungen im Bereich des Schutzes der Privatsphäre enthalten – auf, allen europäischen Bürgern die gleichen gesetzlichen Sicherheiten für den Schutz des Privatlebens und des Briefgeheimnisses zu gewährleisten;

4. fordert die Mitgliedstaaten der Europäischen Union auf, eine europäische Plattform, bestehend aus Vertretern der nationalen Organisationen zu schaffen, die dafür zuständig sind, die Einhaltung der Grund- und Bürgerrechte durch die Mitgliedstaaten zu überwachen, um zu überprüfen, inwieweit die nationalen Rechtsvorschriften im Hinblick auf die Nachrichtendienste mit der Regelung der EMRK und der Charta der Grundrechte der Europäischen Union im Einklang stehen, um die gesetzlichen Regelungen zur Gewährleistung von Brief- und Fernmeldegeheimnis zu überprüfen und um sich überdies auf eine Empfehlung an die Mitgliedstaaten betreffend die Ausarbeitung eines Entwurfs eines Verhaltenskodex zu verständigen, der den Schutz der Privatsphäre, so wie er in Artikel 7 der Europäischen Charta der Grundrechte definiert ist, allen europäischen Bürgern auf dem Staatsterritorium der Mitgliedstaaten in seiner Gesamtheit gewährleistet und darüber hinaus garantiert, dass die Tätigkeit der Nachrichtendienste grundrechtskonform erfolgt, somit den in Kapitel 8 des Berichts seines nichtständigen Ausschusses, insbesondere in Abschnitt 8.3.4, aus Artikel 8 EMRK abgeleiteten Bedingungen entspricht; unterstreicht die Notwendigkeit, gemeinsame Normen zu erarbeiten, die den Erfordernissen des Grundrechtschutzes der Bürger besser angepasst sind und über die Garantien des Artikel 8 EMRK hinausgehen;

5. fordert die Mitgliedstaaten auf, die Charta der Grundrechte der Europäischen Union auf der nächsten Regierungskonferenz als verbindliches und einklagbares Recht zu verabschieden, um so den Grundrechtsschutzstandard, insbesondere im Hinblick auf den Schutz der Privatsphäre, zu erhöhen;

6. ersucht die Mitgliedstaaten des Europarats, ein Zusatzprotokoll zu beschließen, das den Europäischen Gemeinschaften den Beitritt zur EMRK ermöglicht, oder über andere Maßnahmen nachzudenken, die Konflikte in der Rechtsprechung zwischen dem Straßburger und dem Luxemburger Gerichtshof ausschließen;

7. fordert unterdessen die EU-Organe auf, in ihrem jeweiligen Zuständigkeits- und Tätigkeitsbereich die in der EMRK und den zugehörigen Protokollen sowie die in der Charta enthaltenen Grundrechte anzuwenden;

8. fordert den Generalsekretär der Vereinten Nationen auf, den verantwortlichen Ausschuss mit der Vorlage von Vorschlägen zu beauftragen, die auf eine Anpassung von Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte, der den Schutz der Privatsphäre garantiert, an die technischen Neuerungen abzielen;

9. hält es für notwendig, eine Übereinkunft zwischen der Europäischen Union und den Vereinigten Staaten auszuhandeln und zu unterzeichnen, nach der jede der beiden Parteien gegenüber der anderen die Vorschriften über den Schutz der Privatsphäre der Bürger und der Vertraulichkeit von Firmenkommunikationen achtet, die für ihre eigenen Bürger und Unternehmen gelten;

10. fordert die USA auf, das Zusatzprotokoll zum Internationalen Pakt über bürgerliche und politische Rechte zu unterzeichnen, damit Individualbeschwerden gegen die USA wegen seiner Verletzung vor dem konventionellen Menschenrechtsausschuss zulässig werden; die einschlägigen amerikanischen Nichtregierungsorganisationen, insbesondere ACLU (American Civil Liberties Union) und EPIC (Electronic Privacy Information Center) werden ersucht, auf die amerikanische Regierung entsprechenden Druck auszuüben;

zu nationalen gesetzgeberischen Maßnahmen zum Schutze von Bürgern und Unternehmen

11. fordert die Mitgliedstaaten nachdrücklich auf, ihre eigenen Rechtsvorschriften über die Tätigkeit von Nachrichtendiensten erforderlichenfalls anzupassen, um sicherzustellen, dass sie mit den Grundrechten, wie sie in der EMRK sowie der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte niedergelegt sind, übereinstimmen;

12. fordert die Mitgliedstaaten auf, dafür zu sorgen, dass ihnen verbindliche Instrumente zur Verfügung stehen, die einen wirksamen Schutz natürlicher und juristischer Personen gegen jede Art des außergesetzlichen Abhörens gewährleisten;

13. fordert die Mitgliedstaaten auf, ein gemeinsames Schutzniveau gegenüber nachrichtendienstlicher Tätigkeit anzustreben und zu diesem Zweck einen Verhaltenskodex (siehe Ziffer 4) auszuarbeiten, der sich am höchsten mitgliedstaatlichen Schutz orientiert, da die von der Tätigkeit eines Auslandsnachrichtendienstes betroffenen Bürger in der Regel die anderer Staaten und daher auch die anderer Mitgliedstaaten sind;

14. fordert die Mitgliedstaaten auf, mit den USA einen Verhaltenskodex, ähnlich dem der Europäischen Union, auszuhandeln;

15. fordert diejenigen Mitgliedstaaten auf, die dies noch nicht getan haben, eine angemessene parlamentarische und richterliche Kontrolle ihrer Geheimdienste zu gewährleisten;

16. fordert den Rat und die Mitgliedstaaten nachdrücklich auf, dringend ein System zur demokratischen Überwachung und Kontrolle der eigenständigen europäischen nachrichtendienstlichen Kapazitäten sowie anderer damit im Zusammenhang stehender und darauf abgestimmter nachrichtendienstlicher Tätigkeiten auf europäischer Ebene einzurichten; schlägt vor, dass das Europäische Parlament im Rahmen dieses Überwachungs- und Kontrollsystems eine wichtige Rolle zugewiesen bekommt;

17. fordert die Mitgliedstaaten auf, ihre Abhöreinrichtungen zu bündeln, um die Wirksamkeit der Europäischen Sicherheits- und Verteidigungspolitik (ESVP) in den Bereichen nachrichtendienstliche Tätigkeiten, Terrorismusbekämpfung, Weiterverbreitung von Kernwaffen oder internationaler Drogenhandel unter Achtung der Vorschriften über den Schutz der Privatsphäre der Bürger und die Vertraulichkeit von Firmenkommunikationen unter der Kontrolle des Europäischen Parlaments, des Rates und der Kommission zu stärken;

18. fordert die Mitgliedstaaten auf, ein Abkommen mit Drittstaaten zum Zwecke des stärkeren Schutzes der Privatsphäre der EU-Bürger zu schließen, in dem sich alle Vertragstaaten verpflichten, bei Abhörmaßnahmen eines Vertragstaates in einem anderen Vertragstaat letzteren über die geplanten Maßnahmen zu unterrichten;

zu besonderen rechtlichen Maßnahmen zur Bekämpfung der Wirtschaftsspionage

19. fordert die Mitgliedstaaten auf, Überlegungen anzustellen, inwieweit durch Regelungen im europäischen und internationalen Recht Wirtschaftsspionage und Bestechung zum Zweck der Auftragsbeschaffung bekämpft werden können, insbesondere ob eine Regelung im Rahmen der WTO möglich wäre, die der wettbewerbsverzerrenden Wirkung eines derartigen Vorgehens Rechnung trägt, z. B. indem sie die Nichtigkeit solcher Verträge festlegt; fordert die Vereinigten Staaten, Australien, Neuseeland und Kanada auf, sich dieser Initiative anzuschließen;

20. fordert die Mitgliedstaaten auf, sich zu verpflichten, eine Klausel mit dem Verbot von Wirtschaftsspionage in den EG-Vertrag aufzunehmen und keine Wirtschaftsspionage gegeneinander weder direkt oder hinter der Fassade einer ausländischen Macht, die auf ihrem Boden tätig werden könnte, zu betreiben, noch es einer ausländischen Macht zu gestatten, Spionageoperationen vom Boden eines EU-Mitgliedstaates aus zu führen, und damit im Einklang mit dem Geiste und den Bestimmungen des EG-Vertrags zu handeln;

21. fordert die Mitgliedstaaten auf, sich in einem eindeutigen und verbindlichen Dokument selbst zu verpflichten, keine Wirtschaftsspionage zu betreiben, und damit ihren Einklang mit dem Geiste und den Bestimmungen des EG-Vertrags zu signalisieren; fordert die Mitgliedstaaten ferner auf, dieses verbindliche Prinzip in ihre einzelstaatlichen Rechtsvorschriften über Nachrichtendienste zu übernehmen;

22. fordert die Mitgliedstaaten und die Regierung der Vereinigten Staaten auf, einen offenen Dialog zwischen den Vereinigten Staaten und der Europäischen Union über Wirtschaftsspionage einzuleiten;

zu Maßnahmen in Rechtsanwendung und ihrer Kontrolle

23. appelliert an die nationalen Parlamente, die über keine eigenen parlamentarischen Kontrollorgane zur Überwachung der Nachrichtendienste verfügen, solche einzurichten;

24. ersucht die nationalen Kontrollausschüsse der Geheimdienste, bei der Ausübung der ihnen übertragenen Kontrollbefugnisse dem Schutz der Privatsphäre großes Gewicht beizumessen, unabhängig davon, ob es um die Überwachung eigener Bürger, anderer EU-Bürger oder Drittstaatler geht;

25. fordert die Mitgliedstaaten auf, zu gewährleisten, dass ihre Nachrichtendienste nicht zur Erlangung von Wettbewerbsinformationen missbraucht werden, da dies gegen die Pflicht der Mitgliedstaaten zu loyalen Zusammenarbeit und gegen das Konzept eines auf freiem Wettbewerb basierenden Gemeinsamen Marktes verstoßen würde;

26. appelliert an Deutschland und das Vereinigte Königreich, die weitere Gestattung von Abhören von Kommunikation durch Nachrichtendienste der USA auf ihrem Gebiet davon abhängig zu machen, dass diese im Einklang mit der EMRK stehen, d. h. dass sie dem Verhältnismäßigkeitsgrundsatz genügen, ihre Rechtsgrundlage zugänglich und die Wirkung für den Einzelnen absehbar ist, sowie dass eine entsprechend effiziente Kontrolle besteht, da sie für die Menschenrechtskonformität genehmigter oder auch nur geduldeter nachrichtendienstlicher Tätigkeit auf ihrem Territorium verantwortlich sind;

zu Maßnahmen zur Förderung des Selbstschutzes von Bürgern und Unternehmen

27. fordert die Kommission und die Mitgliedstaaten auf, ihre Bürger und Unternehmen über die Möglichkeit zu informieren, dass ihre international übermittelten Nachrichten unter bestimmten Umständen abgefangen werden; besteht darauf, dass diese Information begleitet wird von praktischer Hilfe bei der Entwicklung und Umsetzung umfassender Schutzmaßnahmen, auch was die Sicherheit der Informationstechnik anbelangt;

28. fordert die Kommission, den Rat und die Mitgliedstaten auf, eine wirksame und effektive Politik betreffend die Sicherheit in der Informationsgesellschaft zu entwickeln und umzusetzen; besteht darauf, dass im Rahmen dieser Politik der stärkeren Sensibilisierung aller Nutzer moderner Kommunikationssysteme für Notwendigkeit und Möglichkeiten des Schutzes vertraulicher Informationen besondere Beachtung zukommt; besteht ferner auf der Schaffung eines europaweiten koordinierten Netzes von Agenturen, die in der Lage sind, praktische Hilfe bei der Planung und Umsetzung umfassender Schutzstrategien zu gewähren;

29. ersucht die Kommission und die Mitgliedstaaten, geeignete Maßnahmen für die Förderung, Entwicklung und Herstellung von europäischer Verschlüsselungstechnologie und -software auszuarbeiten und vor allem Projekte zu unterstützen, die darauf abzielen, benutzerfreundliche Kryptosoftware, deren Quelltext offen gelegt ist, zu entwickeln;

30. fordert die Kommission und die Mitgliedstaaten auf, Softwareprojekte zu fördern, deren Quelltext offen gelegt wird, da nur so garantiert werden kann, dass keine „backdoors" eingebaut sind (sog. „open-source Software");

31. fordert die Kommission auf, eine Qualifikation für die Sicherheit von Software festzulegen, die für den Austausch von Nachrichten auf elektronischem Wege bestimmt ist, nach der Software, deren Quellcode nicht offen gelegt ist, in die Kategorie „am wenigsten vertrauenswürdig" eingestuft wird;

32. appelliert an die europäischen Institutionen sowie an die öffentlichen Verwaltungen der Mitgliedstaaten, Verschlüsselung von E-Mails systematisch einzusetzen, um so langfristig Verschlüsselung zum Normalfall werden zu lassen;

33. fordert die gemeinschaftlichen Organe und die öffentlichen Verwaltungen der Mitgliedstaaten auf, dafür zu sorgen, dass ihre Bediensteten ausgebildet und in entsprechenden

Praktika und Ausbildungskursen mit den neuen Technologien und Techniken zur Verschlüsselung vertraut gemacht werden;

34. fordert, dass der Position der Bewerberländer besondere Aufmerksamkeit gewidmet wird; ersucht um Unterstützung, falls sie aufgrund fehlender technologischer Unabhängigkeit nicht für die erforderlichen Schutzmaßnahmen sorgen können;

zu anderen Maßnahmen

35. appelliert an die Unternehmen, mit den Spionageabwehreinrichtungen stärker zusammenzuarbeiten, ihnen insbesondere Attacken von Außen zum Zwecke der Wirtschaftsspionage bekannt zu geben, um so die Effizienz der Einrichtungen zu erhöhen;

36. fordert die Kommission auf, eine Sicherheitsanalyse erstellen zu lassen, aus der hervorgeht, was geschützt werden muss, sowie ein Konzept zum Schutz entwickeln zu lassen;

37. fordert die Kommission auf, ihr Verschlüsselungssystem auf den neuesten Stand zu bringen, da eine Modernisierung dringend notwendig ist, und die Haushaltsbehörde (Rat gemeinsam mit dem Parlament), die dafür erforderlichen Mittel bereitzustellen;

38. schlägt vor, dass sein zuständiger Ausschuss, einen Initiativbericht verfasst, der die Sicherheit und den Geheimschutz bei den europäischen Institutionen zum Inhalt hat;

39. fordert die Kommission auf, den Datenschutz bei der eigenen Datenverarbeitung zu gewährleisten und den Geheimschutz von nicht öffentlich zugänglichen Dokumenten zu intensivieren;

40. ersucht die Kommission und die Mitgliedstaaten, im Rahmen des Sechsten Forschungsrahmenprogramms in neue Technologien der Ent- und Verschlüsselungstechnik zu investieren;

41. dringt darauf, dass die geschädigten Staaten bei Wettbewerbsverzerrungen infolge staatlicher Beihilfen oder aufgrund des Missbrauchs des Systems zur Wirtschaftsspionage die Behörden und Kontrollgremien des Staates, von dessen Hoheitsgebiet aus die Aktivitäten durchgeführt werden, darüber unterrichten, damit die störenden Aktivitäten eingestellt werden;

42. fordert die Kommission auf, einen Vorschlag zur Schaffung – in enger Zusammenarbeit mit der Industrie und den Mitgliedstaaten – eines europaweiten koordinierten Netzes von Beratungsstellen für Fragen der Sicherheit von Unternehmensinformation – insbesondere in den Mitgliedstaaten, in denen derartige Zentren noch nicht bestehen – vorzulegen, das neben der Steigerung des Problembewusstseins auch praktische Hilfestellungen zur Aufgabe hat;

43. hält es für sinnvoll, einen übereuropäischen Kongress zum Schutz der Privatsphäre vor Telekommunikationsüberwachung zu organisieren, um für Nichtregierungsorganisationen aus Europa, den USA und anderen Staaten eine Plattform zu schaffen, wo grenzüberschreitende und internationale Aspekte diskutiert und Tätigkeitsfelder und Vorgehen koordiniert werden können;

o

o o

44. beauftragt seine Präsidentin, diese Entschließung dem Rat, der Kommission, dem Generalsekretär und der Parlamentarischen Versammlung des Europarates, den Regierungen und Parlamenten der Mitgliedstaaten und Beitrittsländer, den Vereinigten Staaten von Amerika, Australien, Neuseeland und Kanada zu übermitteln.