Resolução do Parlamento Europeu sobre a existência de um sistema global de intercepção de comunicações privadas e comerciais (sistema de intercepção "ECHELON") (2001/2098 (INI)) - 05.09.01

O Parlamento Europeu,

- Tendo em conta a sua Decisão de 5 de Julho de 2000 relativa à constituição de uma comissão temporária sobre o sistema de intercepção "ECHELON" , bem como o mandato cometido à referida comissão,

- Tendo em conta o Tratado CE, que visa, inter alia, a realização de um mercado comum caracterizado por um elevado grau de competitividade,

- Tendo em conta os artigos 11º e 12º do Tratado da União Europeia, que sujeitam os Estados-Membros à obrigação de reforçarem e de desenvolverem a solidariedade política mútua,

- Tendo em conta o Tratado da União Europeia, em particular o nº 2 do artigo 6º, que estabelece o compromisso da UE de respeitar os direitos fundamentais, e o Título V, que estabelece disposições relativas à política externa e de segurança comum,

- Tendo em conta o artigo 12º da Declaração Universal dos Direitos do Homem,

- Tendo em conta a Carta dos Direitos Fundamentais da UE, cujo artigo 7º prevê o respeito da vida privada e familiar e consagra expressamente o direito ao respeito das comunicações e cujo artigo 8º prevê a protecção dos dados de carácter pessoal,

- Tendo em conta a Convenção Europeia dos Direitos do Homem, em particular o artigo 8º, que protege a vida privada e a confidencialidade da correspondência, e as numerosas convenções internacionais que estabelecem a protecção da vida privada,

- Tendo em conta os trabalhos realizados pela Comissão Temporária sobre o Sistema de Intercepção ECHELON, a qual levou a cabo inúmeras audições e reuniões com peritos de todo o género e, em particular, com responsáveis dos sectores público e privado da esfera das telecomunicações e da protecção de dados, com pessoal dos serviços de informações, jornalistas e advogados peritos na matéria, deputados dos parlamentos nacionais dos Estados-Membros, etc.,

- Tendo em conta o nº 2 do artigo 150º do seu Regimento,

- Tendo em conta o relatório da Comissão Temporária sobre o Sistema de Intercepção ECHELON (A5-0264/2001),

A. Considerando não existirem já quaisquer dúvidas quanto à existência de um sistema global de intercepção de comunicações que opera graças à cooperação entre os EUA, o Reino Unido, o Canadá, a Austrália e a Nova Zelândia no âmbito do acordo UKUSA; que, com base nos indícios existentes e em inúmeras declarações coincidentes provenientes de um vasto leque de pessoas e organizações - inclusive de fontes americanas -, parece provável que o seu nome é efectivamente ECHELON, embora isso constitua um pormenor de somenos,

B. Considerando que já não podem existir dúvidas de que o sistema visa, no mínimo, interceptar comunicações privadas e comerciais, mas não comunicações militares, embora a análise levada a efeito no relatório tenha revelado que as capacidades técnicas do sistema não são provavelmente tão poderosas como, em parte, o haviam suposto os meios de comunicação,

C. Considerando ser, por conseguinte, espantoso, para não dizer preocupante, que inúmeros responsáveis comunitários ouvidos pela Comissão Temporária, nomeadamente Comissários europeus, tenham declarado não ter conhecimento deste fenómeno,

Os limites do sistema de intercepção

D. Considerando que o sistema de intercepção se baseia, em particular, na intercepção global de comunicações via satélite, embora em zonas de elevada densidade de comunicações só uma parte extremamente reduzida das mesmas seja efectuada por satélite; que, por isso, a maior parte das comunicações não pode ser interceptada por estações terrestres, mas sim unicamente através de ligações por cabo e de escuta via rádio, o que - tal como o demonstram as investigações efectuadas no âmbito do presente relatório - só é possível dentro de limites estritos; que o volume de efectivos necessário para a análise e a avaliação das comunicações interceptadas impõe outras limitações; que, por conseguinte, os Estados UKUSA só têm acesso a uma proporção muito reduzida das comunicações por cabo e por rádio e só podem analisar e avaliar uma proporção ainda mais reduzida das mesmas; que, além disso, por muito vastos que sejam os meios disponíveis e as capacidades de intercepção de comunicações, o elevadíssimo número das mesmas torna impossível, na prática, o controlo exaustivo e pormenorizado de todas as comunicações,

A eventual existência de outros sistemas de intercepção

E. Considerando que a intercepção de comunicações constitui um método de espionagem tradicional dos serviços de informações e que um sistema desta natureza também poderia ser explorado por outros países, desde que dispusessem dos necessários recursos financeiros, bem como das condições geográficas requeridas; que a França, graças aos seus territórios ultramarinos, é o único Estado-Membro da UE que reúne as condições geográficas e técnicas para operar de forma autónoma um sistema global de intercepção e que dispõe também da infra-estrutura técnica e organizativa para o fazer; que existem igualmente fortes indícios de que também a Rússia explora provavelmente um tal sistema,

Compatibilidade com o Direito Comunitário

F. Considerando que, no tocante à questão da compatibilidade de um sistema do tipo ECHELON com o Direito Comunitário, há que proceder à seguinte distinção: se o sistema só for utilizado para fins de informação, não há qualquer violação do direito da UE; uma vez que as actividades dos serviços de segurança do Estado não são abrangidas pelo Tratado CE, embora o fossem pelo Título V do TUE (PESC), que, porém, actualmente não contém disposições sobre a matéria, pelo que não se dispõe de critérios aplicáveis; se, pelo contrário, o sistema for abusivamente utilizado para fins de espionagem da concorrência, tal acção será contrária à obrigação de lealdade dos Estados-Membros e à concepção de um mercado comum assente na livre concorrência, razão pela qual um Estado-Membro que nele participe viola o Direito Comunitário,

G. Considerando as declarações feitas pelo Conselho na sessão plenária de 30 de Março de 2000, segundo as quais o Conselho não pode aceitar a criação ou a existência de um sistema de intercepção das telecomunicações que não respeite as regras de Direito dos Estados-Membros e que viole os princípios fundamentais destinados a salvaguardar a dignidade humana,

Compatibilidade com o direito fundamental ao respeito pela vida privada (artigo 8º CEDH)

H. Considerando que toda e qualquer intercepção de comunicações representa um atentado grave ao exercício do direito à vida privada; que o art. 8º da CEDH, que garante o respeito da vida privada, permite a interferência com o exercício desse direito apenas para garantir a segurança nacional, desde que tal esteja previsto em disposições do direito nacional que sejam acessíveis a todos e estabeleçam as circunstâncias e condições em que o Estado a pode exercer; que, além disso, tal ingerência deve ser proporcionada, pelo que deve ser feita uma ponderação dos interesses concorrentes, e que, em conformidade com a jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH), não é suficiente que a ingerência seja meramente útil ou desejável,

I. Considerando que um sistema de informações que interceptasse de forma aleatória e permanente todas as comunicações violaria o princípio da proporcionalidade e não seria compatível com a CEDH; que, do mesmo modo, se as disposições reguladoras do controlo das comunicações não tivessem base legal, se não fossem acessíveis ao público ou se a sua formulação fosse de molde a não permitir prever as suas implicações para o indivíduo, ou ainda se essa intercepção não fosse proporcionada, tal constituiria também uma violação da CEDH; que as disposições nos termos das quais os serviços de informações norte-americanos operam no estrangeiro são, na sua maioria, secretas, pelo que o respeito do princípio da proporcionalidade é, pelo menos, questionável e se observa provavelmente uma violação dos princípios da acessibilidade do direito e da previsibilidade dos seus efeitos, princípios esses estabelecidos pelo TEDH,

J. Considerando que os Estados-Membros não podem eximir-se aos compromissos que lhes são impostos pela CEDH, deixando operar no seu território os serviços de informações de outros Estados sujeitos a disposições legais menos rigorosas, uma vez que, de outro modo, o princípio da legalidade e as suas duas componentes - acessibilidade e previsibilidade - perderiam o seu efeito e a jurisprudência do TEDH seria privada de substância,

K. Considerando, além disso, que a conformidade das operações legais dos serviços de informações com os direitos fundamentais implica a existência de sistemas de controlo adequados, a fim de contrabalançar os riscos inerentes a actividades secretas por parte da Administração; que o Tribunal Europeu dos Direitos do Homem salientou expressamente a importância de um sistema de controlo eficaz da actividade dos serviços de informações e que, por conseguinte, se afigura preocupante que alguns Estados-Membros não disponham de quaisquer órgãos de controlo parlamentar dos respectivos serviços secretos,
A questão de saber se os cidadãos da UE estarão suficientemente protegidos contra os serviços de informações

L. Considerando que a protecção dos cidadãos da UE depende da situação jurídica observada em cada um dos Estados-Membros, mas que são consideráveis as diferenças registadas e que, em alguns casos, se verifica mesmo a ausência de órgãos de controlo parlamentares, pelo que dificilmente pode ser considerada suficiente a protecção existente; que os cidadãos europeus têm

um interesse fundamental em que os respectivos parlamentos nacionais sejam dotados de uma comissão de controlo específica, formalmente estruturada, que vigie e controle a actividade dos serviços de informações; que, todavia, mesmo onde existem tais órgãos de controlo, grande é a tentação de votar maior atenção às actividades internas dos serviços de informações do que às actividades externas, uma vez que, regra geral, os cidadãos nacionais apenas são visados no primeiro caso; que, se os serviços de informações fossem obrigados a notificar *a posteriori* um cidadão cujas comunicações tivessem sido interceptadas, por exemplo, decorridos cinco anos após essa intercepção, tal constituíria um incentivo à prática da intercepção proporcionada,

M. Considerando que, face à sua dimensão, não podem ser construídas no território de um país estações de recepção de comunicações por satélite sem o seu consentimento,

N. Considerando que, em caso de cooperação entre serviços de informações no âmbito da PESC ou da JAI, cumpre às instituições promover a introdução de medidas adequadas a proteger os cidadãos europeus,

Espionagem industrial

O. Considerando que constitui parte integrante das atribuições dos serviços de informações no estrangeiro a recolha de dados económicos, como sejam o desenvolvimento de sectores específicos, a evolução dos mercados das matérias-primas, a observância de embargos, o respeito das disposições relativas ao aprovisionamento de bens de utilização dual, etc., e que, por essa razão, as empresas que desenvolvem actividades nesses domínios são, frequentemente, vigiadas,

P. Considerando que os serviços de informações dos EUA não investigam apenas factos de interesse económico geral, mas interceptam também pormenorizadamente comunicações entre empresas, sobretudo no quadro da adjudicação de contratos, justificando essa intercepção com o propósito de combater tentativas de corrupção; que, no caso de uma intercepção pormenorizada, existe o risco de as informações não serem utilizadas para a luta contra a corrupção, mas sim para a espionagem dos concorrentes, ainda que os EUA e o Reino Unido declarem que não o fazem; que, no entanto, o papel do 'Advocacy Center' do Ministério do Comércio dos EUA continua a não estar cabalmente esclarecido e que foi cancelada uma reunião que havia sido agendada para esclarecer precisamente esta questão,

Q. Considerando que a OCDE adoptou, em 1997, uma Convenção sobre a luta contra a corrupção de agentes públicos, a qual prevê a punição criminal, a nível internacional, da corrupção, pelo que, também por esse motivo, a prática de actos de corrupção não pode justificar a intercepção de comunicações;

R. Considerando que a situação se torna intolerável quando os serviços de informações se deixam instrumentalizar para efeitos de espionagem da concorrência, espiando empresas estrangeiras para lograr vantagens concorrenciais para empresas nacionais; que, embora se afirme com frequência que o sistema global de intercepção tem sido utilizado para esse efeito, não existem, no entanto, provas factuais que o atestem,

S. Considerando que, durante a visita efectuada aos EUA por uma delegação da Comissão Temporária, fontes autorizadas confirmaram o relatório Brown do Congresso dos EUA, referindo que 5% das informações recolhidas a partir de fontes não declaradas são utilizadas para fins de espionagem económica; que as mesmas fontes calculam que essa actividade de

controlo de informações poderia permitir à indústria norte-americana obter contratos num valor que pode atingir os 7 mil milhões de dólares;

T. Considerando que os dados comerciais sensíveis se encontram, fundamentalmente, no interior das empresas, pelo que a espionagem consiste, nomeadamente, na tentativa de obter informações através dos próprios funcionários ou de pessoas infiltradas e, cada vez mais, penetrando nas respectivas redes informáticas; que apenas nos casos em que dados sensíveis são transmitidos para o exterior via cabo ou via rádio (satélite) é possível utilizar um sistema de vigilância das comunicações para fins de espionagem da concorrência, e que tal se aplica sistematicamente aos três casos seguintes:
- a empresas que operam em três fusos horários, de tal modo que os resultados intercalares podem ser enviados da Europa para a América e, seguidamente, para a Ásia;
- a videoconferências de empresas multinacionais realizadas via satélite ou por cabo;
- a negociações de contratos importantes in loco (construção de infra-estruturas, infra-estruturas de telecomunicações, criação de novos sistemas de transporte, etc.) que requeiram contactos com a sede da empresa em causa,

U. Considerando que a sensibilização das pequenas e médias empresas para os riscos e as questões de segurança é muitas vezes insuficiente, pelo que tais empresas não reconhecem os perigos da espionagem económica nem da intercepção de comunicações,

V. Considerando que nem sempre existe um sentido de segurança muito desenvolvido nas Instituições europeias (à excepção do Banco Central Europeu, da Direcção-Geral do Conselho para as Relações Externas e da Direcção-Geral da Comissão para as Relações Externas), pelo que se torna necessário empreender acções neste domínio,
Possibilidades de autoprotecção

W. Considerando que as empresas só podem considerar-se em segurança se protegerem todo o seu ambiente de trabalho, bem como todos os meios de comunicação que sirvam para transmitir informações sensíveis; que são em número suficiente os sistemas de cifragem seguros existentes a preços módicos no mercado europeu; que também as pessoas singulares devem ser incentivadas a cifrar o respectivo correio electrónico, uma vez que um correio não cifrado equivale a uma carta sem envelope; que, na Internet, se encontram sistemas relativamente conviviais, postos à disposição de todas as pessoas, por vezes mesmo gratuitamente,
Cooperação entre os serviços de informações no interior da UE

X. Considerando que a UE chegou a acordo quanto à coordenação da recolha de informações pelos serviços de informações no âmbito do desenvolvimento da sua própria política de defesa e de segurança comum, embora prossiga a cooperação com outros parceiros nestes domínios,

Y. Considerando que o Conselho Europeu decidiu em Helsínquia, em Dezembro de 1999, desenvolver uma capacidade militar europeia mais eficaz, a fim de poder dar cumprimento a todas as missões estabelecidas em Petersberg no contexto da PESC; que o Conselho Europeu decidiu, além disso, que a União, a fim de concretizar este objectivo até 2003, deveria estar habilitada a destacar rapidamente forças militares compostas por 50.000 a 60.000 pessoas, tropas essas auto-suficientes e que disponham das necessárias capacidades de comando, controlo e informações secretas; que os primeiros passos rumo à criação de uma tal capacidade autónoma em matéria de informações já foram dados no quadro da UEO e do Comité permanente político e de segurança,

Z. Considerando que a cooperação entre os serviços de informações existentes na UE se afigura indispensável, uma vez que, por um lado, uma política de segurança comum que excluísse os serviços secretos seria absurda e que, por outro, tal comportaria inúmeras vantagens de ordem profissional, financeira e política; que tal seria, além disso, conforme à ideia de uma parceria assente na igualdade de direitos com os Estados Unidos e seria susceptível de reunir todos os Estados-Membros no seio de um sistema instituído na plena observância da Convenção Europeia dos Direitos do Homem; que o controlo correspondente por parte do Parlamento Europeu deverá, ser nesse caso assegurado,

AA. Considerando que o Parlamento Europeu está a implementar o Regulamento (CE) nº 1049/2001 do Parlamento Europeu e do Conselho, de 30 de Maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão[(2)] mediante a adaptação das disposições do seu Regimento respeitantes ao acesso a documentos sensíveis,

Conclusão e alteração de acordos internacionais sobre a protecção dos cidadãos e empresas

1. Afirma, com base nas informações obtidas pela Comissão Temporária, que não subsistem dúvidas quanto à existência de um sistema de intercepção mundial de comunicações que opera com a participação dos Estados Unidos, do Reino Unido, do Canadá, da Austrália e da Nova Zelândia, ao abrigo do acordo UKUSA;

2. Insta o Secretário-Geral do Conselho da Europa a apresentar ao Comité de Ministros uma proposta tendente a proteger a vida privada, protecção esta consagrada no artigo 8º da CEDH, em sintonia com métodos de comunicação e de intercepção modernos, por meio de um protocolo adicional ou, juntamente com as disposições relativas à protecção de dados, aquando de uma revisão da Convenção relativa à Protecção de Dados, na condição de que tal não se traduza, nem numa redução do nível de protecção estabelecido pelo Tribunal Europeu dos Direitos do Homem, nem numa redução da flexibilidade necessária para ter em conta futuras evoluções,

3. Solicita aos Estados-Membros - cujas leis que regulamentam o poder de intercepção dos serviços secretos criam discriminações em matéria de protecção da privacidade - que assegurem a todos os cidadãos europeus as mesmas garantias legais relativas à protecção da vida privada e ao carácter confidencial da correspondência;

4. Exorta os Estados-Membros da União Europeia a instituírem uma plataforma europeia, composta por representantes dos órgãos nacionais responsáveis pelo controlo do desempenho dos Estados-Membros em matéria de direitos fundamentais e cívicos, a fim de examinar a conformidade das legislações nacionais relativas aos serviços de informações com a CEDH e com a Carta dos Direitos Fundamentais da UE, a reverem as disposições legais relativas à garantia da confidencialidade da correspondência e das comunicações, e a chegarem a acordo quanto a uma recomendação destinada aos Estados-Membros sobre a elaboração de um código de conduta que garanta a todos os cidadãos europeus, no território dos Estados-Membros, a protecção da vida privada, tal como definida no artigo 7º da Carta dos Direitos Fundamentais da UE, e que, sobretudo, assegure que as actividades dos serviços de informações se processem no respeito dos direitos fundamentais e em conformidade com as condições enunciadas no capítulo 8 do relatório da Comissão Temporária do Parlamento Europeu, em particular no ponto 8.3.4, baseado no artigo 8º da CEDH; salienta a necessidade de elaborar normas comuns mais

adaptadas às exigências de protecção dos direitos fundamentais dos cidadãos da União, normas que sejam mais vastas do que as garantidas pelo artigo 8º da CEDH;

5. Convida os Estados-Membros a adoptarem, na próxima Conferência Intergovernamental, a Carta dos Direitos Fundamentais da UE enquanto instrumento jurídico vinculativo e susceptível de ser invocado em juízo, por forma a promover o nível de protecção dos direitos fundamentais, em particular no que respeita à protecção da vida privada;

6. Insta os Estados-Membros do Conselho da Europa a adoptarem um protocolo adicional que possibilite a adesão das Comunidades Europeias à CEDH ou a reflectirem sobre outras medidas tendentes a prevenir conflitos de competência entre o Tribunal Europeu dos Direitos do Homem e o Tribunal de Justiça das Comunidades Europeias;

7. Insta, entretanto, as Instituições da UE a aplicarem, no âmbito dos respectivos poderes e competências, os direitos fundamentais consagrados na CEDH e nos protocolos anexos, bem como na Carta;

8. Exorta o Secretário-Geral da ONU a incumbir a comissão responsável de apresentar propostas que visem a adaptação do artigo 17º do Pacto Internacional sobre os Direitos Civis e Políticos, que garante a protecção da vida privada, ao progresso técnico;

9. Considera essencial a negociação e a assinatura de uma convenção entre a União Europeia e os EUA que estabeleça que cada uma das partes respeitará, relativamente à outra, as disposições relativas à protecção da vida privada dos cidadãos e à confidencialidade das comunicações das empresas que são aplicáveis aos seus próprios cidadãos e empresas;

10. Insta os EUA a assinarem o Protocolo Adicional ao Pacto Internacional sobre os Direitos Civis e Políticos, a fim de tornar admissíveis as queixas apresentadas por particulares por violação do mesmo por parte dos EUA junto da Comissão dos Direitos do Homem prevista na Convenção; exorta as ONG americanas pertinentes, em particular a ACLU (American Civil Liberties Union) e a EPIC (Electronic Privacy Information Center) a exercerem pressões nesse sentido junto do governo norte-americano;

Disposições legais nacionais de protecção dos cidadãos e empresas

11. Exorta os Estados-Membros a reverem e, se necessário, adaptarem a sua própria legislação sobre a actividade dos serviços de informações, a fim de assegurarem a respectiva conformidade com os direitos fundamentais, tal como consagrados na CEDH e na jurisprudência do Tribunal Europeu dos Direitos do Homem;

12. Convida os Estados-Membros a dotarem-se de instrumentos vinculativos que garantam uma protecção eficaz das pessoas singulares e colectivas contra toda e qualquer forma de intercepção ilegal das suas comunicações;

13. Insta os Estados-Membros a diligenciarem no sentido de um nível de protecção comum face à actividade dos serviços de informações e a elaborarem para esse efeito um código de conduta (tal como referido no nº 4) que se norteie pelo nível de protecção mais elevado que existente nos Estados-Membros, uma vez que os cidadãos afectados pela actividade de um serviço de informações externas são, em geral, cidadãos de outros Estados e, por conseguinte, também de outros Estados-Membros;

14. Convida os Estados-Membros a negociarem com os EUA um código de conduta semelhante ao da UE;

15. Convida os Estados-Membros que ainda o não tenham feito a assegurarem um controlo parlamentar e judicial adequado dos respectivos serviços secretos;

16. Exorta o Conselho e os Estados-Membros a conferirem prioridade ao estabelecimento de um sistema de supervisão e de controlo democráticos da capacidade europeia autónoma de recolha de informações, bem como de outras actividades comuns e coordenadas de recolha de informações a nível europeu; sustenta que o Parlamento Europeu deve protagonizar um importante papel nesse sistema de supervisão e controlo;

17. Convida os Estados-Membros a conjugarem os respectivos meios de intercepção das comunicações, no intuito de reforçar a eficácia da PESD nos domínios dos serviços de informações, da luta contra o terrorismo, da proliferação nuclear ou do tráfico internacional de estupefacientes, no respeito das disposições relativas à protecção da vida privada dos cidadãos e à confidencialidade das comunicações das empresas, sob o controlo do Parlamento Europeu, do Conselho e da Comissão;

18. Exorta os Estados-Membros a concluírem um acordo com países terceiros na perspectiva do reforço da protecção da vida privada dos cidadãos da UE, nos termos do qual todas as partes contratantes se comprometam a, em caso de intercepção praticada por uma das partes no território de outra, informar a segunda sobre as medidas previstas;

Medidas legais específicas de combate à espionagem económica

19. Exorta os Estados-Membros a estudarem em que medida a espionagem industrial e o suborno para fins de obtenção de contratos poderiam ser combatidos mediante disposições do direito europeu e internacional e, em particular, se seria possível adoptar regulamentação no âmbito da OMC que tivesse em conta o impacto de uma tal actividade em termos de distorção da concorrência, determinando, por exemplo, a nulidade dos contratos obtidos dessa forma; exorta os Estados Unidos, a Austrália, a Nova Zelândia e o Canadá a participarem nesta iniciativa;

20. Exorta os Estados-Membros a incluírem no Tratado CE uma cláusula que proíba a espionagem industrial, a comprometerem-se a não a praticar uns contra os outros, directamente ou a coberto de uma potência estrangeira susceptível de operar no seu território, nem a permitir a esta última a realização de operações de espionagem a partir do território de um Estado-Membro da UE, por forma a observarem o espírito e a letra do Tratado CE;

21. Exorta os Estados-Membros a inserirem na alínea g) do artigo 3º do Tratado CE uma menção explícita da ilegalidade da espionagem industrial mútua e a patentearem desse modo a sua conformidade com o espírito e a letra do Tratado CE; exorta os Estados-Membros a transporem este princípio vinculativo para as respectivas legislações nacionais aplicáveis aos serviços de informações;

22. Exorta os Estados-Membros e o Governo dos EUA a encetarem um diálogo aberto EUA-UE sobre a recolha de informações económicas;

Medidas de aplicação da lei e respectivo controlo

23. Insta os parlamentos nacionais que não disponham de um órgão parlamentar de controlo dos serviços de informações a procederem à respectiva criação;

24. Insta os órgãos nacionais de controlo das actividades dos serviços secretos a atribuírem grande importância à protecção da vida privada, no exercício das suas funções de controlo, independentemente de os cidadãos visados serem cidadãos nacionais, cidadãos de outros Estados-Membros da UE ou cidadãos de países terceiros;

25. Exorta os Estados-Membros a diligenciarem no sentido de garantir que os seus sistemas de informações não sejam abusivamente utilizados para fins de recolha de informações em matéria de concorrência, contrariando o dever de lealdade dos Estados-Membros e o conceito de um mercado comum assente na livre concorrência;

26. Apela à Alemanha e ao Reino Unido para que, no futuro, subordinem a autorização de operações de intercepção de comunicações, no seu território, pelos serviços de informações dos EUA, à observância do disposto na CEDH, ou seja, para que estabeleçam que tais actividades deverão ser conformes ao princípio da proporcionalidade, que a sua base legal deverá ser acessível a todos, devendo os seus efeitos para o indivíduo ser previsíveis, e instituam as devidas medidas de controlo,uma vez que lhes cabe assegurar que as operações desenvolvidas pelos serviços de informações no seu território sejam consentâneas com o respeito dos direitos do Homem, independentemente de as operações em causa serem autorizadas ou meramente toleradas;

Medidas de incremento da autoprotecção de cidadãos e empresas

27. Insta a Comissão e os Estados-Membros a informarem os seus cidadãos e as suas empresas sobre a possibilidade de as respectivas comunicações internacionais poderem, em determinadas circunstâncias, ser interceptadas; reitera que esta informação deve ser acompanhada por assistência prática na concepção e implementação de medidas globais de protecção, incluindo a segurança das tecnologias da informação;

28. Insta a Comissão, o Conselho e os Estados-Membros a desenvolverem e implementarem uma política eficaz e activa em prol da segurança na Sociedade da Informação; insiste em que, no quadro desta política, se deverá votar particular atenção ao reforço da sensibilização de todos os utilizadores de modernos sistemas de comunicações para a necessidade da protecção de informações confidenciais; reitera, além disso, a necessidade de criar, à escala europeia e de forma coordenada, uma rede de organismos capazes de prestar assistência prática na concepção e aplicação de estratégias globais de protecção;

29. Insta a Comissão e os Estados-Membros a elaborarem medidas adequadas à promoção, ao desenvolvimento e à produção de tecnologias e "software" de cifragem europeus e a apoiarem, sobretudo, projectos que visem o desenvolvimento de "software" de cifragem de código-fonte aberto e de fácil utilização;

30. Insta a Comissão e os Estados-Membros a promoverem projectos de "software" de código-fonte aberto ("open-source software"), pois só assim se poderá garantir que não tenha lugar a integração de "backdoors" nos programas;

31. Convida a Comissão a definir uma qualificação do nível de segurança dos pacotes de "software" de correio electrónico, colocando na categoria menos fiável todo o "software" cujo código-fonte não seja aberto;

32. Apela às Instituições europeias e às administrações públicas dos Estados-Membros para que pratiquem sistematicamente a cifragem do correio electrónico, por forma a que, a longo prazo, a cifrahem se torne regra habitual;

33. Solicita às Instituições comunitárias e às administrações públicas dos Estados-Membros que promovam a formação do seu pessoal e a familiarização do mesmo com as novas tecnologias e técnicas de cifragem mediante a realização dos estágios e cursos de formação necessários;

34. Requer que seja dispensada uma atenção particular à situação dos países candidatos; solicita que lhes seja prestada assistência, caso os mesmos não possam implementar as medidas de protecção necessárias devido a um défice de independência tecnológica;

Outras medidas

35. Exorta as empresas a cooperarem de forma mais estreita com os serviços de contra-espionagem, informando-os, em particular, de quaisquer ataques provenientes do exterior para fins de espionagem industrial, de modo a aumentar a eficácia desses serviços;

36. Exorta a Comissão a providenciar no sentido da realização de uma análise em matéria de segurança que revele aquilo que tem de ser protegido, e a desenvolver uma estratégia de protecção;

37. Exorta a Comissão a actualizar o seu sistema de cifragem de acordo com o nível técnico mais recente, já que é premente uma modernização, e insta a autoridade orçamental (Conselho, juntamente com o Parlamento) a disponibilizar os recursos necessários para o efeito;

38. Propõe que a sua comissão competente elabore um relatório de iniciativa que incida na segurança e na protecção da condidencialidade nas Instituições europeias;

39. Insta a Comissão a garantir a protecção dos dados nos seus próprios sistemas de processamento e a intensificar a protecção das informações confidenciais em relação a documentos que não sejam acessíveis ao público;

40. Exorta a Comissão e os Estados-Membros a investirem, no âmbito do 6º Programa-Quadro de Investigação, em novas tecnologias de descodificação e de codificação;

41. Insta a que, em caso de distorção da concorrência causada por auxílios estatais ou por espionagem industrial abusiva, os países prejudicados informem as autoridades e os órgãos de controlo do país a partir de cujo território essas acções tenham sido levadas a cabo, a fim de se pôr de termo a tais actividades de distorção;

42. Exorta a Comissão a apresentar uma proposta que, em estreita cooperação com a indústria e com os Estados-Membros, estabeleça uma rede europeia e coordenada de centros de consultoria - em particular nos Estados-Membros em que tais centros ainda não existam - sobre questões relacionadas com a segurança das informações detidas por empresas, a qual, a par do aumento da sensibilização para o problema, tenha também como missão proporcionar ajuda prática;

43. Considera conveniente a organização de um congresso internacional sobre a protecção da vida privada face à vigilância das telecomunicações, a fim de criar uma plataforma que permita às ONG da Europa, dos EUA e de outros Estados debater os aspectos transfronteiriços e internacionais do problema e coordenar domínios de actividades e procedimentos;

44. Encarrega a sua Presidente de transmitir a presente resolução ao Conselho, à Comissão, ao Secretário-Geral e à Assembleia Parlamentar do Conselho da Europa e aos governos e parlamentos dos Estados-Membros e dos países candidatos à adesão, dos Estados Unidos da América, da Austrália, da Nova Zelândia e do Canadá.