Parecer do Comité Económico e Social Europeu sobre a «Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social Europeu e ao Comité das Regiões — Estratégia para uma sociedade da informação segura — Diálogo, parcerias e maior poder de intervenção»

COM(2006) 251 final

(2007/C 97/09)

Em 31 de Maio de 2006, a Comissão decidiu, nos termos do artigo 262.º do Tratado que institui a Comunidade Europeia, consultar o Comité Económico e Social Europeu sobre a proposta supramencionada.

A Secção Especializada de Transportes, Energia, Infra-estruturas e Sociedade da Informação, encarregada de preparar os correspondentes trabalhos, emitiu parecer em 11 de Janeiro de 2007, sendo relator **A. PEZZINI**.

Na 433.ª reunião plenária de 15 e 16 de Fevereiro de 2007 (sessão de 16 de Fevereiro), o Comité Económico e Social Europeu adoptou, por 132 votos a favor, sem votos contra e 2 abstenções, o seguinte parecer:

1. **Conclusões e recomendações**

1.1 O Comité está convicto de que o problema da segurança informática é uma preocupação crescente não só para as empresas, as administrações, os organismos públicos e privados, como também para os cidadãos individuais.

1.2 O Comité partilha, em linhas gerais, as análises e os argumentos a favor de uma nova estratégia para aumentar a segurança das redes e da informação contra os ataques e as intrusões que transcendem as fronteiras geográficas.

1.3 Dada a amplitude do fenómeno e as suas consequências no plano económico e na vida privada, a Comissão deveria, na opinião do Comité, redobrar esforços para elaborar uma estratégia inovadora e articulada.

1.3.1 Sublinha, além disso, que a Comissão publicou ainda recentemente uma nova comunicação sobre a segurança informática e que está anunciado para breve um novo documento sobre o mesmo tema. O Comité reserva-se a possibilidade de exprimir-se futuramente a este propósito, num parecer mais articulado, sobre estas comunicações.

1.4 Na opinião do Comité, a vertente da segurança informática não deverá ser de forma alguma dissociada do reforço da protecção dos dados pessoais e da salvaguarda da liberdade, que são direitos consagrados pela Convenção Europeia dos Direitos Humanos.

1.5 O CESE pergunta-se qual será, na situação actual, o valor acrescentado da proposta em relação à abordagem integrada de 2001, cujo propósito coincide com o da presente comunicação [1].

1.5.1 O documento de avaliação de impacto [2], anexo à proposta, contém algumas actualizações importantes em relação à posição adoptada em 2001, mas foi publicado numa única versão linguística, não sendo por isso acessível a muitos cidadãos europeus que têm normalmente a possibilidade de ajuizar sobre o documento oficial redigido em todas línguas comunitárias.

1.6 O Comité recorda as conclusões da Cimeira Mundial sobre a sociedade da informação, realizada na Tunísia em 2005, subscritas pela Assembleia da ONU em 27 de Março de 2006:

— acesso não discriminatório,

— promoção das TIC como instrumento de paz,

— definição de instrumentos para reforçar a democracia, a coesão e a boa governação,

— prevenção dos abusos em relação aos direitos humanos [3].

1.7 O Comité entende que uma estratégia comunitária dinâmica e integrada poderia abordar, para além do diálogo, das parcerias e de um maior poder de intervenção, os temas seguintes:

— acções de prevenção,

— a transição da segurança informática para a garantia da informação [4],

— a elaboração de um quadro comunitário seguro e reconhecido juridicamente, regulamentar e com um regime de sanções,

— o reforço da normalização técnica,

---

[1] Ver parecer CESE sobre a Comunicação da Comissão ao Conselho, Parlamento Europeu, Comité Económico e Social e Comité das Regiões — Segurança das redes e da informação: Proposta de abordagem de uma política europeia, JO C 48 de 21.12.2002, p. 3.

[2] Um «documento de impacto» não tem o mesmo valor de um «documento de estratégia».

[3] ONU 27.3.2006, Recomendação n.os 57 e 58. Documento final da Tunísia, n. 15.

[4] Ver *Emerging technologies in the context of security* CCR — Instituto de protecção e segurança do cidadão, caderno de investigação estratégica, Comissão Europeia, http://serac.jrc.it.

— a identificação digital dos utilizadores,

— o lançamento de exercícios europeus de análise e de prospectiva sobre a segurança informática, em condições de convergência tecnológica multimodal,

— o reforço dos mecanismos europeus e nacionais de avaliação dos riscos,

— acções destinadas a impedir a emergência de monoculturas informáticas,

— o reforço da coordenação comunitária ao nível europeu e internacional,

— a instituição de um ponto de contacto «Segurança TIC» (*Security Focal Point*), comum a várias direcções-gerais,

— a criação de uma rede europeia para a segurança das redes e da informação (*European Network and Information Security Network*),

— a optimização do papel da investigação europeia na segurança informática,

— a proclamação de um «Dia europeu do computador seguro»,

— a organização nas escolas de vários tipos e graus de acções-piloto comunitárias sobre questões de segurança informática.

1.8 O Comité considera, por último, que uma estratégia comunitária dinâmica e integrada carece de dotações financeiras orçamentais adequadas, com iniciativas e acções de coordenação reforçadas ao nível comunitário, capazes de representar a Europa, a uma única voz, no palco mundial.

2. **Justificação**

2.1 É fundamental fazer face aos desafios colocados pela segurança da sociedade da informação para garantir a confiança e a fiabilidade das redes e dos serviços de comunicação, factores determinantes para o desenvolvimento da economia e da sociedade.

2.2 Urge proteger as redes e os sistemas informáticos para manter as suas capacidades competitivas e comerciais, assegurar a integridade e a continuidade das comunicações electrónicas, para prevenir a fraude e garantir a protecção jurídica da privacidade.

2.3 As comunicações electrónicas e os serviços conexos representam o segmento mais amplo de todo o sector das telecomunicações: em 2004 cerca de 90 % das empresas europeias utilizaram activamente a Internet e 65 % delas desenvolveram um sítio individual na Internet, calculando-se que cerca de metade da população europeia recorre regularmente à Internet e que 25 % das famílias utilizam sistematicamente a banda larga de acesso ([5]).

2.4 Não obstante o desenvolvimento acelerado dos investimentos, o volume das despesas com a segurança representam apenas uma percentagem situada entre os 5 e 13 % do total dos investimentos nas tecnologias de informação. Ora, esta percentagem é realmente exígua. Estudos recentes evidenciaram que «numa média de 30 protocolos que partilham as mesmas estruturas-chave, 23 são vulneráveis a ataques multiprotocolo» ([6]). Além disso, calcula-se que se eleva a 25 milhões a média das mensagens electrónicas *spam* ([7]) enviadas diariamente. O Comité regozija-se, por isso, com a recente proposta da Comissão que trata deste assunto.

2.5 No âmbito dos vírus informáticos ([8]), a difusão rápida e em larga escala de «*worms*» ([9]) e de «*spyware*» ([10]) tem acompanhado o desenvolvimento incessante de sistemas e de redes de comunicação electrónica. Estes são cada vez mais complexos e, ao mesmo tempo, vulneráveis, também devido à convergência de multimédia e telefonia móvel, bem como dos sistemas *GRID infoware* ([11]): os casos de extorsão, DdoS (*Distributed denials of service*), furto de identidade em linha, *phishing* ([12]), pirataria ([13]), etc. representam igualmente enormes desafios para a segurança da sociedade da informação. A Comunidade Europeia já analisou este fenómeno em comunicação de 2001 ([14]) sobre a qual o Comité teve a oportunidade de pronunciar-se ([15]), propondo agora uma estratégia com três linhas de intervenção:

— medidas de segurança específicas,

([5]) Para uma abordagem dinâmica de uma sociedade da informação segura. DG Sociedade da informação e meios de comunicação, «Factsheet 8» (Junho de 2006) http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

([6]) *Proceedings of the First International Conference on Availability, Reliability and Security* (ARES'06) — volume 00 ARES 2006 Editor: IEEE Computer Society.

([7]) *Spam* = mensagens comerciais por correio electrónico não desejadas. *Spam* significava originalmente «*spiced pork and ham*», uma espécie de conserva de carne em gelatina muito popular durante a Segunda Guerra Mundial quando se transforma no principal alimento das tropas americanas e da população do Reino Unido. Depois de anos a fio com este regime alimentar, o termo adquiriu fatalmente uma conotação negativa.

([8]) *Vírus informático*: um vírus é um programa malicioso desenvolvido por programadores que, como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios. A maioria das contaminações ocorrem pela acção do utilizador executando o anexo de um e-mail. A segunda causa de contaminação é por Sistema Operacional desactualizado, sem a aplicação de correctivos que bloqueiam chamadas maliciosas nas portas do computador. (www. wikipedia.org/wiki/Virus_informatico).

([9]) Vírus informático (*worm*): um vírus é um programa malicioso capaz de reproduzir-se a si próprio: um vírus *e-mail* representa um ataque devastador a uma rede informática por recolher todos os endereços e-mail contidos num programa local (por exemplo, MS Outlook) e enviá-los seguidamente a centenas de e-mail que passam a conter o mesmo vírus como anexo invisível.

([10]) Software espião (*spyware*) = programas de software que registam os dados de navegação dos utilizadores e se instalam automaticamente sem o conhecimento, o consentimento e o controlo deste.

([11]) *GRID infoware* (Computação em grade): é um modelo computacional capaz de alcançar uma alta taxa de processamento dividindo geograficamente as tarefas entre diversas máquinas (p.ex. supercomputador, sistemas de memorização de dados, fontes de dados, instrumentos e pessoas), apresentando-as como recurso único apto a resolver cálculos de extrema complexidade e processamento de dados de carácter particularmente intensivo.

([12]) *Phishing*: é um tipo de fraude electrónica projectada para roubar informações valiosas pessoais e confidenciais com a finalidade de furto de identidade mediante a utilização de mensagens de correio electrónico falsas, criadas com a intenção de passarem por autênticas.

([13]) Pirataria: é um termo utilizado pelos «piratas da Internet» para descrever um software a que foi retirada a protecção auto-cópia e que fica disponível para ser recarregado via Internet.

([14]) COM(2001) 298 final.

([15]) Ver nota 1.

— quadro regulamentar, incluindo a protecção de dados e da privacidade,

— luta contra a cibercriminalidade.

2.6 O levantamento dos ataques informáticos e a sua identificação e prevenção, no âmbito de um sistema em rede, são um desafio para a busca de soluções adequadas, face às mudanças constantes de configuração, à variedade de protocolos de rede e de serviços prestados e desenvolvidos e ainda à extrema complexidade dos comportamentos assíncronos de ataque ([16]).

2.7 Mas, infelizmente, a escassa visibilidade do rendimento do investimento em segurança e, no caso dos cidadãos, o facto de não estarem conscientes da sua responsabilidade na cadeia de segurança global, levaram a subestimar os riscos e a diminuir a atenção dedicada ao desenvolvimento de uma cultura de segurança.

3. **A proposta da Comissão**

3.1 Com a sua comunicação sobre a estratégia para uma sociedade da informação segura ([17]), a Comissão pretende melhorar a segurança informática através de uma estratégia dinâmica e integrada, baseada

a) na melhoria do diálogo entre as autoridades públicas e a Comissão, com a aferição de desempenhos das políticas nacionais e a identificação das práticas mais eficazes de comunicação electrónica de um modo seguro;

b) na sensibilização das PME e dos cidadãos para a necessidade de sistemas de segurança eficazes, com um papel activo de estímulo da Comissão e o maior envolvimento da Agência Europeia de Segurança das Redes e da Informação (AESRI/ /ENISA);

c) no diálogo sobre os instrumentos regulamentares para alcançar um equilíbrio social adequado entre segurança e protecção dos direitos fundamentais, incluindo a privacidade.

3.2 Além disso, a comunicação prevê, na perspectiva do estabelecimento de um quadro adequado para a recolha de dados sobre os incidentes de segurança, sobre os níveis de confiança dos utilizadores e sobre as tendências da indústria da segurança, uma parceria baseada na confiança da ENISA

a) com os Estados-Membros

b) com os consumidores e os utilizadores,

c) com a indústria da segurança informática,

d) com o sector privado,

mediante a criação de um portal comunitário multilingue que apresente informação, adaptada às necessidades dos destinatários, sobre ameaças, riscos e alertas, com o fito de estabelecer uma parceria estratégica com o sector privado, os Estados-Membros e a comunidade dos investigadores.

3.2.1 Preconiza, por outro lado, um maior poder de intervenção de cada grupo de interessados que permita conhecer melhor as necessidades e os riscos em termos de segurança.

3.2.2 No atinente à cooperação internacional, e especificamente com os países terceiros, «a dimensão mundial da segurança das redes e da informação exige que a Comissão, a nível internacional e em coordenação com os Estados-Membros, intensifique os seus esforços para promover a cooperação mundial neste domínio» ([18]), mas esta observação não é tida em conta nas acções de diálogo, parceria e responsabilização.

4. **Observações**

4.1 O Comité concorda com as análises e com os argumentos que justificam uma estratégia europeia integrada e dinâmica para a segurança das redes e da informação. A questão da segurança é, a seu ver, fundamental se se pretende fomentar uma atitude mais propícia à aplicação das TIC e melhorar a confiança nelas. As posições do Comité foram já, aliás, ilustradas por numerosos pareceres ([19]).

4.1.1 Volta a salientar ([20]) que «a rede Internet e as novas tecnologias da comunicação em linha (por exemplo, os telemóveis ou os computadores de bolso com ligação Internet e funções multimédia, em grande desenvolvimento) constituem, aos olhos do Comité, instrumentos fundamentais para o desenvolvimento da economia do conhecimento, da e-economia e da e-administração».

([16]) *Multivariate Statistical Analysis for Network Attacks Detection*. Guangzhi Qu, Salim Hariri*- 2005 USA, Arizona — Internet Technology Laboratory, ECE Department, The University of Arizona, http://www.ece.arizona.edu/~hpdc Mazin Yousif, Intel Corporation, USA — Trabalho financiado, em parte, pela Intel Corporation IT R&D Council.

([17]) COM(251) 2006 final de 31.05.06.

([18]) Ver COM (2006) 251 final — capítulo 3, penúltimo parágrafo.

([19]) São os seguintes:
— Parecer do CESE sobre a «*Proposta de directiva do Parlamento Europeu e do Conselho relativa à conservação de dados tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis e que altera a Directiva 2002/58/CE*», JO C 69 de 21.3.2006, p. 16
— Parecer do CESE sobre a «*Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre i2010 — Uma sociedade da informação europeia para o crescimento e o emprego*», JO C 110 de 9.5.2006, p. 83
— Parecer do CESE 1651 sobre a «*Proposta de decisão do Parlamento Europeu e do Conselho que adopta um programa comunitário plurianual para a promoção de uma utilização mais segura da Internet e das novas tecnologias em linha*», JO C 157 de 28.6.2005, p. 136
— Parecer do CESE sobre a «*Comunicação da Comissão ao Conselho, Parlamento Europeu, Comité Económico e Social e Comité das Regiões — Segurança das redes e da informação: Proposta de abordagem de uma política europeia*», JO C 48 de 21.2.2002, p. 3.

([20]) Ver nota 19, 3.º travessão.

4.2 *Adopção pela Comissão de propostas mais enérgicas*

4.2.1 O Comité reputa, todavia, essencial ampliar a abordagem proposta pela Comissão, que consiste em basear essa estratégia comunitária dinâmica e integrada num diálogo aberto e inclusivo, bem como em parcerias e num maior poder de intervenção, por forma a envolver todas as partes interessadas e, em particular, os utilizadores.

4.2.2 Esta posição já havia sido defendida em pareceres anteriores: «Esta luta deve também dizer directamente respeito, para ser eficaz, a todos os utilizadores da Internet, que devem ser formados e informados das precauções a tomar e dos meios a utilizar para se prevenirem contra a recepção desses conteúdos perigosos ou não desejáveis, ou para não serem utilizados como transmissores desses conteúdos. A parte informação e formação do plano de acção deve, segundo o Comité, dar prioridade elevada à mobilização dos utilizadores […]» ([21]).

4.2.3 Na opinião do Comité, os utilizadores e os cidadãos devem ser envolvidos mas com a preocupação de conciliar a necessária protecção dos dados e das redes com as liberdades cívicas e o direito dos utilizadores a acessos seguros a preços módicos.

4.2.4 Convém ter em mente que a busca de segurança informática representa um custo suplementar para o consumidor, também em termos de tempo perdido para remover ou contornar os obstáculos. O Comité pensa que conviria estabelecer a obrigação de uma combinação automática de sistemas de protecção anti-vírus em todos os computadores, a activar ou não pelos utilizadores mas fazendo parte do produto na origem.

4.3 *Uma estratégia comunitária mais dinâmica e inovadora*

4.3.1 Além disso, o Comité defende que a União deveria fixar objectivos mais ambiciosos e gizar uma estratégia inovadora, integrada e dinâmica com o lançamento de novas iniciativas. Como, por exemplo:

— mecanismos que permitam a identificação digital de cada um dos utilizadores, vezes de mais convidados a fornecer os seus dados anagráficos;

— acções, por intermédio do ETSI ([22]), que representam um requisito para uma utilização segura das TIC e que ofereçam soluções pontuais e rápidas, com um limiar comum de segurança em toda a União;

— acções de prevenção, através da integração dos requisitos mínimos de segurança nos sistemas informáticos e de rede e o lançamento de acções-piloto prevendo a organização de cursos de segurança nas escolas de todos os tipos e graus;

— criação de um quadro comunitário seguro e juridicamente reconhecido; este quadro, aplicado à informática e às redes, permitiria transitar da segurança informática para o seguro informático;

— o reforço dos mecanismos europeus e nacionais de avaliação dos riscos e uma melhor capacidade de aplicação das disposições legislativas e regulamentares para atacar os crimes informáticos perpetrados contra a privacidade e os arquivos de dados;

— acções destinadas a impedir a emergência de monoculturas informáticas com produtos e soluções mais fáceis de «piratear»; apoio a inovações multiculturais diversificadas para a realização de um Espaço Único Europeu da Informação (SEIS — *Single European Information Space*).

4.3.2 No entender do Comité, seria oportuno criar um ponto de contacto «*Segurança das TIC*» inter-DG ([23]), que permitiria actuar

— ao nível dos serviços da Comissão;

— ao nível dos vários Estados-Membros, através de soluções horizontais no atinente aos aspectos de interoperacionalidade, gestão da identidade, protecção da privacidade, liberdade de acesso à informação e aos serviços e requisitos mínimos de segurança;

— ao nível internacional, para que a UE possa falar a uma só voz nos vários contextos internacionais, como a ONU, o G8, a OCDE e a ISO.

4.4 *Reforço das acções comunitárias de coordenação responsável*

4.4.1 O Comité confere também grande importância à criação de uma rede europeia para a segurança das redes e da informação que promoveria inquéritos, estudos e *workshops* sobre mecanismos de segurança e a sua interoperacionalidade, sobre criptografia avançada e sobre a protecção da privacidade.

4.4.2 O Comité considera oportuno, num sector tão delicado, optimizar o papel da investigação europeia mediante uma síntese adequada do conteúdo

— do programa europeu de investigação sobre a segurança (ESRP) ([24]), retomado no 7.ºPrograma-Quadro de RDT;

([21]) Ver nota 19, 3.º travessão.

([22]) ETSI (Instituto Europeu de Normas de Telecomunicações), em particolar, o Workshop de 16 e 17 de Janeiro de 2006. O ETSI elaborou, designadamente, especificações sobre as interceptações ilegais (TS 102 232; 102 233; 102 234, sobre acessos Internet Lan Wireless (TR 102 519), sobre assinaturas electrónicas, tendo desenvolvido algoritmos de segurança para GSM GPRS e UMTS.

([23]) Este ponto de contacto poderia ser financiado no âmbito das prioridades TSI do programma específico de cooperação 7.º Programma--quadro IDT ou pelo programma europeu de investigação sobre a segurança ESRP.

([24]) Ver Programa-Quadro CE de IDT&D, Programa específico «Cooperação»; prioridade temática «investigação sobre segurança» com um orçamento de 1,35 mil milhões de euros para o período 2007-2013.

— do programa *Safer Internet Plus*;

— do programa europeu de protecção das infra-estruturas críticas (PEPIC) ([25]).

4.4.3 A estas sugestões poder-se-ia aduzir a proclamação de um «Dia Europeu do Computador Seguro», secundado por campanhas nacionais de educação nas escolas e de informação dos consumidores sobre procedimentos de protecção das informações pelo computador. Isso para além, obviamente, das informações que dizem respeito aos progressos tecnológicos registados no mundo dos computadores, muito vasto e em constante mutação.

4.4.4 O Comité sublinhou já por várias vezes que «a rapidez com que as empresas estão dispostas a introduzir as TIC nas suas actividades comerciais depende da concepção que tiverem da segurança das transacções em linha e do sentimento de confiança que inspiram. O grau de confiança dos consumidores determina em grande medida a vontade de revelar o seu número de cartão de crédito numa página Internet» ([26]).

4.4.5 O Comité está convicto de que o enorme potencial de crescimento do sector exigirá, por um lado, políticas específicas e, por outro, a adequação das políticas actuais aos novos desenvolvimentos. No âmbito de uma estratégia integrada, haverá que interligar as iniciativas de segurança informática, removendo as fronteiras sectoriais e garantindo a difusão homogénea e segura das TIC na sociedade.

4.4.6 A seu ver, há estratégias fundamentais, como a presente, que avançam com demasiada lentidão em virtude de entraves burocráticos e culturais colocados pelos Estados-Membros às decisões indispensáveis que são tomadas obrigatoriamente ao nível comunitário.

4.4.7 O Comité é igualmente de opinião que os recursos comunitários são insuficientes para pôr em marcha os múltiplos e urgentes projectos capazes de dar uma resposta concreta aos novos problemas da globalização, na condição de serem realizados à escala comunitária.

4.5 *Maiores garantias comunitárias na protecção dos consumidores*

4.5.1 O Comité está ciente de que os Estados-Membros adoptaram medidas tecnológicas de segurança e procedimentos de gestão da segurança em função das próprias exigências mas focando, tendencialmente, aspectos diversos. Este é um dos motivos por que se torna tão difícil fornecer uma resposta unívoca e eficaz aos problemas de segurança. À excepção de algumas redes administrativas, não há uma cooperação transfronteiriça sistemática entre os Estados-Membros, não obstante a consciência de que as questões de segurança não podem ser resolvidas isoladamente por cada país.

4.5.2 O Comité observa, além disso, que o Conselho instaurou, com a sua decisão-quadro 2005/222/JAI, um sistema de cooperação entre as autoridades judiciárias e as demais autoridades competentes dos Estados-Membros para garantir que estes adoptem uma abordagem coerente, aproximando as suas legislações penais em matéria de ataques aos sistemas de informação no âmbito

— do acesso ilegal aos sistemas de informação,

— da interferência ilegal no sistema, mediante acto intencional e não autorizado de impedir ou interromper gravemente o funcionamento de um sistema de informação,

— da interferência ilegal nos dados, mediante acto intencional de apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis os dados informáticos de um sistema de informação,

— da instigação, auxílio, cumplicidade e tentativa de prática de alguma das infracções acima referidas.

4.5.3 Além disso, a decisão-quadro propõe critérios para a determinação da responsabilidade da pessoa colectiva e fixar as eventuais sanções a aplicar nos casos em que a responsabilidade desta última é declarada ([27]).

4.5.4 O Comité aprova a proposta da Comissão de procurar, como primeiro passo, melhorar o diálogo entre as autoridades públicas, lançando um exercício de aferição de desempenhos das políticas nacionais relacionadas com a SRI, incluindo políticas de segurança específicas para o sector público. Esta sugestão tinha, aliás, já sido feita pelo Comité em parecer de 2001.

4.6 *Generalização da cultura de segurança*

4.6.1 No que se refere ao envolvimento da indústria de segurança informática, esta deverá garantir realmente, para defender o direito dos seus clientes à privacidade e à confidencialidade dos seus dados pessoais, a utilização de sistemas de vigilância material das suas instalações e da codificação das comunicações, adequados à evolução tecnológica ([28]).

([25]) COM(2005) 576 final de 17.11.2005.
([26]) Ver nota 19, 2.º travessão.
([27]) Ver nota 19, 4.º travessão.
([28]) Ver Directiva 97/66/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações (JO L 24 de 30.01.1998, p. 1-8.

4.6.2 No atinente às acções de sensibilização, o Comité reputa fundamental a instauração de uma verdadeira «cultura de segurança», concebida de uma forma inteiramente compatível com a liberdade de informação, de comunicação e de expressão. Recorda, por outro lado, que há muitos utilizadores que não estão conscientes de todos os riscos associados à pirataria informática e muitos operadores, vendedores e prestadores de serviços que não têm capacidade para avaliar os pontos mais vulneráveis do sistema e a sua amplitude.

4.6.3 Se a protecção da vida privada e dos dados pessoais é um objectivo prioritário, os consumidores têm, do mesmo modo, direito a ser protegidos com eficácia contra a obtenção abusiva de perfis pessoais conseguida através de programas de espionagem (*spyware* e *webug*) ou outros meios. A prática de *spamming* ([29]) (envio maciço de mensagens não solicitadas), que decorre muitas vezes destes abusos deveria também ser eficazmente travada. Estas intrusões prejudicam as vítimas ([30]).

4.7 *Uma agência europeia mais forte e mais activa*

4.7.1 O Comité veria com bons olhos que Agência Europeia de Segurança das Redes e da Informação (ENISA) tivesse um papel mais incisivo e reforçado quer no âmbito das acções de sensibilização quer, sobretudo, das acções de informação e formação dos operadores e utilizadores, conforme preconiza, aliás, o seu recente parecer ([31]) sobre a oferta de serviços de comunicações electrónicas publicamente disponíveis.

4.7.2 Com respeito, por último, às acções propostas de responsabilização de cada grupo de interessados, estas parecem relevar de uma estrita observância do princípio da subsidiariedade. Com efeito, cabe aos Estados-Membros e ao sector privado a sua concretização em função das suas responsabilidades específicas.

4.7.3 A ENISA deveria tirar partido dos contributos da rede europeia para a segurança das redes e da informação para a organização de actividades conjuntas, bem como do portal comunitário na Internet multilingue de segurança informática para informação personalizada e interactiva, com uma linguagem fácil tendo sobretudo como alvo o utilizador individual de faixas etárias diversas e nas pequenas e médias empresas.

Bruxelas, 6 de Fevereiro de 2007.

O Presidente
do Comité Económico e Social Europeu
Dimitris DIMITRIADIS

([29]) Pollu postage, em francês.

([30]) Ver Pareceres do CESE sobre os temas: redes de comunicações electrónicas (JO C 123 de 25.4.2001, pág. 50), *Comércio electrónico* (JO C 169 de 16.6.1999, p. 36) e *Efeitos do comércio electrónico no mercado único* (JO C 123 de 25.04.2001, p. 1).

([31]) Ver nota 19, 1.º travessão.