Parecer do Comité Económico e Social 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»

(2002/C 48/07)

Em 7 de Junho de 2001, a Comissão Europeia decidiu, nos termos do artigo 262.º do Tratado que institui a Comunidade Europeia, consultar o Comité Económico e Social sobre a comunicação supramencionada.

Incumbida da preparação dos correspondentes trabalhos, a Secção de Transportes, Energia, Infra-estruturas e Sociedade da Informação adoptou parecer em 6 de Novembro de 2001, sendo relator D. Retureau.

Na 386.ª reunião plenária de 28 e 29 de Novembro de 2001 (sessão de 28 de Novembro), o Comité Económico e Social adoptou por 113 votos a favor, 2 votos contra e 3 abstenções o seguinte parecer.

1. Introdução

1.1. O desenvolvimento das redes internas nas empresas, administrações e outros organismos, bem como as ligações destes e dos particulares à Internet prossegue a um ritmo exponencial. Não fosse o próximo desenvolvimento da Internet rápida [1] e a introdução de um novo sistema de atribuição de nomes de domínios de primeiro nível, rapidamente se atingiria a saturação.

1.2. A sociedade, a economia, a administração, a segurança nacional, civil e militar, dependem cada vez mais do bom funcionamento e da fiabilidade das redes e das suas interligações, da largura de banda e da integridade da informação que contêm e, em muitos casos, da confidencialidade dos dados e da exacta identificação das pessoas envolvidas.

1.3. A segurança das redes e das comunicações é, a partir de agora, uma questão estratégica da maior importância que necessita de uma política coordenada e coerente a nível dos Estados-Membros da União e a nível global.

1.4. A comunicação da Comissão analisa com muito pormenor e, na opinião do Comité, boa fundamentação, os problemas e a situação existentes e apresenta propostas de acção.

2. As propostas da Comissão

2.1. A comunicação da Comissão apresenta uma abordagem comum das questões de segurança das redes e da transmissão de informação na Europa. Trata-se de promover um nível equivalente de protecção em todos os Estados-Membros, a interoperabilidade dos sistemas, as funções de segurança pública indispensáveis na Internet e o papel regulador dos Estados-Membros.

2.2. O objectivo é garantir uma espécie de «serviço mínimo» de segurança nas redes, nas ligações dos particulares à Internet e nas interligações das redes, bem como desenvolver uma cultura da segurança que promova a sensibilização geral para os problemas e as suas soluções.

2.3. O elo mais fraco determina a segurança do todo e a introdução gradual de ligações de alta velocidade (ADSL, cabo) e da ligação permanente à Internet, incluindo de particulares, gera novas exigências de protecção. O mesmo se diga do comércio electrónico, onde os dados pessoais e as referências de pagamento dos consumidores devem ser protegidos, do mesmo modo que os dados pessoais dos cidadãos devido à evolução da e-administração.

2.4. É também necessário um quadro penal suficientemente harmonizado para que os delitos de intrusão, desvio de dados e informação, controlo de redes por piratas ou disseminação voluntária de vírus tenham definições e sanções equivalentes em todos os países.

2.5. A Comissão propõe a criação de um sistema europeu de alerta e intervenção e insiste na necessidade de formação e informação para as empresas e os particulares, sendo este o ponto central da comunicação.

[1] Norma Ipv6 que permite 6 000 milhões de endereços IP.

2.6. Por fim, a proposta centra-se no objectivo prioritário da protecção da vida privada e da confidencialidade dos dados pessoais dos cidadãos e dos consumidores.

3. **Observações do CES**

3.1. *Observações na generalidade*

3.1.1. O Comité concorda plenamente com as análises e argumentos que justificam um quadro político europeu de segurança das redes e da informação e, na generalidade, considera as propostas pertinentes, sob reserva de algumas observações e sugestões específicas.

3.1.2. A rede Internet não foi concebida para o comércio electrónico, os contratos, a venda de conteúdos protegidos pelo direito de autor (música, imagens e filmes), as transferências de capitais e outras operações económicas que exigem segurança específica. Na sua utilização inicial, militar e universitária, a cifragem com chaves longas, no primeiro caso, e a publicação de resultados de experiências ou bases de dados científicos em claro, no segundo, respondiam às necessidades. Até 2000, por razões de segurança nacional, a cifragem robusta era interdita aos particulares em muitos países, essencialmente não europeus, o mesmo acontecendo com a exportação de certos programas. Felizmente, a Comissão deu um impulso ao desenvolvimento e comércio de instrumentos de segurança indispensáveis às empresas e às administrações para a transmissão de dados confidenciais em linha.

3.1.3. Desenvolveu-se depois uma utilização «libertária» da Internet, seguida da utilização comercial, financeira, tecnológica, industrial e lúdica, sem contar os sítios pornográficos que geram importantes receitas e estão na origem, como os jogos em linha, de inovações tecnológicas consideráveis, nomeadamente em matéria de qualidade de imagem e de alta velocidade ou de sistemas de pagamento seguros, anónimos ou não.

3.1.4. Todos estes modos de utilização continuam a coexistir e surgem outros. Partes cada vez mais vastas das redes e da Internet servem de pilar ao funcionamento da sociedade e da economia, contribuem decisivamente para o desenvolvimento social e a segurança nacional e exigem segurança proporcional à natureza dos dados transmitidos e das operações efectuadas, no respeito da vida privada e sem pôr em causa a própria base da Internet, ou seja, a livre circulação de informação e o intercâmbio aberto de dados, ideias, resultados científicos, etc.

3.1.5. Entende o Comité que deverá sempre existir proporcionalidade entre as medidas de segurança adoptadas e o seu custo, a natureza e importância dos dados e operações protegidas e as categorias de utilizadores abrangidas.

3.1.6. O Comité concorda, na generalidade, com os riscos potenciais apresentados e as soluções propostas pela Comissão. Concorda também com o ponto de vista segundo o qual a segurança é uma questão dinâmica que exige adaptação e ajustamentos permanentes em função das evoluções tecnológicas, dos programas informáticos e dos riscos. É por isso que sugere que a consulta e o diálogo iniciados, por ocasião desta comunicação, com as indústrias, os utilizadores e os responsáveis da segurança das redes passem a ser permanentes ou periódicos. A sociedade civil organizada deverá participar plenamente, dado o impacto da política de segurança das redes e das comunicações em certos direitos fundamentais dos cidadãos, nas actividades económicas e sociais e na administração.

3.1.7. Em pareceres recentes sobre «a cibercriminalidade» [1] e a «protecção da infância na Internet» [2], o Comité expôs já os princípios essenciais que defende para lutar contra a utilização da Internet para fins ilícitos ou criminosos, rejeitando a censura, a vigilância generalizada e os entraves à liberdade de expressão e de comunicação na rede global. A Internet, contudo, não está à margem do direito.

3.1.8. O Comité considera que a segurança dos utilizadores individuais e dos consumidores, em todas as suas vertentes, deveria ocupar um lugar mais central na reflexão da Comissão e na estratégia europeia. Ainda que um ataque de vírus contra um computador de um particular não tenha consequências de

---

[1] Parecer sobre a comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões — Criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade (CES 1115/2001) (ainda não publicado no Jornal Oficial).

[2] Parecer do CES, em elaboração, sobre um programa para a protecção dos menores na Internet.

maior do ponto de vista dos interesses económicos directos ou da segurança colectiva, é necessário lembrar que certos ataques em larga escala transitam pelos computadores dos particulares e, por vezes, podem ser empolados pelos media, exagerando o risco real, o que reduz fortemente a confiança dos cidadãos nas vantagens e utilidade da Internet. Isto afecta consideravelmente o potencial de desenvolvimento do comércio electrónico e do e-business em geral e a criação de novos empregos.

3.1.9. Se a protecção da vida privada e dos dados pessoais é objectivo prioritário, os consumidores têm também direito a ser protegidos de maneira realmente eficaz contra a obtenção abusiva de perfis pessoais conseguida através de programas de espionagem (*spyware* e *webug*) ou outros meios. A prática de *spamming* (envio maciço de mensagens não solicitadas) que decorre muitas vezes destes abusos deveria também ser eficazmente travada. Estas intrusões prejudicam as vítimas ([1]).

3.1.10. A protecção da vida privada deve aplicar-se a todas as pessoas que participam na actividade económica e comercial e, por conseguinte, ser alargada aos trabalhadores e outros colaboradores de empresa. As normas internas de segurança devem ser negociadas entre os parceiros sociais e ser bem conhecidas no interior das empresas, no respeito do quadro legal ou jurisprudencial do Estado-Membro. Importa salientar, a este propósito, a importância de uma aplicação uniforme de tais disposições, em conformidade com a Carta dos Direitos Fundamentais adoptada em Nice, e tendo igualmente em atenção a Recomendação dos garantes europeus relativa à vida privada e a Directiva 95/48/CE dobre a protecção dos dados pessoais.

3.1.11. Parece pois indispensável dar aos particulares e às empresas meios jurídicos mais eficazes para exigir responsabilidades financeiras aos operadores e aos fabricantes de programas no caso de deficiências graves de segurança e de protecção de dados que lhes sejam imputáveis, a título de responsabilidade pelos produtos ([2]).

3.1.12. O Comité entende que a Comissão deve dar mais importância e divulgação ao papel positivo, em termos de recursos e de protecção, dos sistemas livres (*open source*), ou seja, os sistemas de exploração e os programas de redes e de comunicação gratuitos e livremente modificáveis pelos utilizadores. A comunidade de programadores de sistemas livres reagiu rapidamente para corrigir as falhas e problemas e em torno desta realidade, apoiada por alguns gigantes da indústria informática, desenvolveu-se um importante sector económico de serviços às empresas. Grande número de servidores no mundo funcionam com estes programas de modo geralmente seguro e estável, ao passo que ocorre por vezes que certos programas patenteados só são corrigidos com um atraso prejudicial aos utilizadores ou que novas versões dos mesmos, com novas funcionalidades, são introduzidas precipitadamente no mercado. As razões de concorrência comercial ou a busca da novidade a todo o custo sobrepõem-se por vezes a uma cultura da segurança, que deve ser mais frequentemente respeitada pelos autores de programas, comerciais ou gratuitos, para que seja efectivamente integrada nos produtos desde a sua concepção.

3.1.13. Por outro lado, os sistemas de gestão e os programas próprios, cujo código-fonte não é publicado, não oferecem, por isso, garantia suficiente de segurança e protecção da vida privada, sobretudo no caso de registo de licenças e carregamento de *patches* (correcções e actualizações) efectuados pela Internet, que podem ser desviados para coligir informação sobre os sistemas cliente e servidor (arquitectura e conteúdos, listas de endereços e ligações). O Comité considera que todas as práticas que vão além do simples registo do nome e morada do titular da licença do programa para lhe dar uma chave de activação ou um código de acesso temporário a serviços constituem uma intrusão e devem ser proibidas.

3.1.14. Os programas informáticos livres (*free*: gratuitos) asseguram também uma forma de sã concorrência face a tendências monopolistas do mercado de programas e do mercado dos serviços de rede em pleno desenvolvimento.

3.1.15. A licença pública geral [GPL ([3])] deve ser reconhecida e respeitada. O Comité considera que deveriam ser desenvolvidas abordagens e regras específicas, em matéria de propriedade intelectual, para os programas e conteúdos cujo acesso e intercâmbio se possam fazer via Internet. É demasiado fácil, por exemplo, utilizar a legislação sobre marcas para entravar o exercício da liberdade de opinião ou de expressão dos consumidores ou dos trabalhadores sobre a política ou as práticas de uma empresa e os seus produtos ou serviços. O direito de patentes e marcas parece encontrar limites e problemas de aplicação face ao desenvolvimento das redes, que requerem, por conseguinte, legislação específica de protecção, ainda insuficientemente elaborada.

([1]) Ver parecer do CES sobre «Redes de comunicações electrónicas» (JO C 123 de 25.4.2001, p. 50), sobre o «Comércio electrónico» (JO C 169 de 16.6.1999, p. 36) e sobre «Os efeitos do comércio electrónico sobre o mercado único» (JO C 123 de 25.4.2001, p. 1).

([2]) Parecer do CES: JO C 117 de 26.4.2001, p. 1.

([3]) (General public licence), licença pública geral que reconhece a propriedade intelectual do autor de um programa informático gratuito.

3.1.16. Por outro lado, tendo em conta que as tentativas de intercepção e de controlo ou roubo de dados sensíveis se efectuam principalmente contra redes militares, administrativas e de empresas, o Comité insta as instituições europeias e todos os Estados-Membros a lutar em conjunto contra todas as intercepções e tentativas de intrusão com fins de espionagem militar, industrial ou comercial, que prejudicam os interesses estratégicos e económicos da Europa, seja qual for a sua origem.

3.1.17. As medidas de segurança, a vigilância dos acessos, as normas e protocolos internos, as redundâncias materiais (sistemas que suprem as avarias, sistemas-espelho e *proxy*, salvaguarda frequente e descentralizada de dados) exigem programas e equipamento informáticos, vigilância e actualização permanente por pessoas muito qualificadas e têm, por consequência, um custo elevado, enquanto que, tanto em razão de insuficiência de informação técnica e de conhecimentos como das suas possibilidades financeiras, especialmente no caso das PME-PMI, elas suscitam grandes problemas de aplicação às empresas públicas e privadas e às administrações. As equipas de alerta de urgência deveriam estar bem equipadas e ter em consideração as necessidades das PME-PMI.

3.2. *Observações na especialidade*

3.2.1. Observações na especialidade sobre os riscos e os meios de luta previstos

3.2.1.1. Protecção da vida privada e luta contra a cibercriminalidade e a espionagem

3.2.1.1.1. O Comité concorda plenamente com a prioridade atribuída na proposta da Comissão à protecção da vida privada e da confidencialidade dos dados pessoais. A protecção dos direitos fundamentais e da liberdade de informação e de comunicação devem constituir o cerne de toda a estratégia em matéria de protecção de dados e de comunicações, assim como a protecção dos interesses colectivos, a começar pela necessidade de assegurar a segurança nacional e o funcionamento normal das instituições democráticas e das administrações públicas. O Comité concorda com a necessidade de desenvolver e adaptar os meios destinados a estes fins, sejam eles legislativos, de cooperação, investigação ou normalização.

3.2.1.1.2. Apesar de dever ser mantida a possibilidade de intercepção legal, no respeito dos processos jurídicos apropriados, os meios de cifragem robusta podem torná-la impossível. A grande criminalidade conhece e utiliza os meios mais modernos e seguros para proteger as suas comunicações. Deve ser desenvolvida uma cooperação jurídica e tecnológica no plano europeu e internacional contra a grande criminalidade e o terrorismo, como o Comité sublinhou, nomeadamente, nos seus pareceres sobre a luta contra o branqueamento de capitais e a cibercriminalidade [1].

3.2.1.1.3. É também indispensável, no quadro da política de concorrência, supervisar os processos de concentração e de monopolização no que respeita aos conteúdos (informação, cultura, ...) e os diversos segmentos dos encaminhadores da espinha dorsal (*backbones*) da Internet. A Comissão deveria velar também pelo estabelecimento de um «governo» da rede mais representativo dos 370 milhões de utilizadores actuais, realmente transparente, já que o actual «governo» multicéfalo está concentrado na América do Norte e sob controlo do Departamento de Comércio dos Estados Unidos, em especial para a atribuição da gestão de nomes de domínio e a escolha de registrars [2].

3.2.1.1.4. Para proteger o direito à vida privada e à confidencialidade dos seus clientes, os operadores devem garantir efectivamente a utilização de meios de vigilância material das suas instalações e de cifragem das comunicações que sejam mais adequados à importância dos direitos a proteger, em função da evolução técnica. Aliás a isso estão obrigados, nomeadamente pela Directiva 97/66/CE [3].

3.2.1.1.5. Os utilizadores, por seu lado, devem poder cifrar de maneira suficientemente segura os dados sensíveis que tenham de transmitir pela rede, mas estão geralmente pouco a par dos meios apropriados disponíveis para cada necessidade concreta e da forma de os aplicar. Para ocorrer às crescentes necessidades de cifrar e de segurança, é indispensável formar especialistas em número suficiente.

3.2.1.1.6. As intrusões em computadores e redes, sejam quais forem as motivações (desafio intelectual, vingança pessoal ou desejo de prejudicar, roubo de informações ou controlo para diversos fins), e a disseminação de vírus informáticos põem em perigo os direitos e interesses dos utilizadores e a integridade dos dados, da informação e da rede.

---

(1) Parecer do CES, em elaboração, sobre um programa para a protecção dos menores na Internet.Ver parecer do CES sobre «Redes de comunicações electrónicas» (JO C 123 de 25.4.2001, p. 50), sobre o «Comércio electrónico» (JO C 169 de 16.6.1999, p. 36) e sobre «Os efeitos do comércio electrónico sobre o mercado único» (JO C 123 de 25.4.2001, p. 1).

(2) Empresas incumbidas da atribuição e gestão de certos nomes de primeiro nível.

(3) Directiva sobre a protecção de dados no sector das telecomunicações (JO L 24 de 30.1.1998).

3.2.1.1.7. Embora plenamente de acordo com a Comissão sobre a importância dos prejuízos que podem causar as diversas formas de intrusão, que podem, por vezes, chegar ao controlo furtivo do sistema, o Comité considera que é excessivo assimilar os *hackers*, que põem em evidência falhas de segurança sem intenção criminosa — o que permite corrigi-las — àqueles que se introduzem nos sistemas para fins ilícitos (*crackers*). A legislação penal que a Comissão venha a propor deve ser proporcional aos crimes e delitos eventuais, que devem ser rigorosamente definidos e qualificados, e ter em consideração a intenção dos autores das intrusões.

3.2.1.2. Direito comunitário aplicável e tecnologias disponíveis

3.2.1.2.1. O direito comunitário obriga os Estados-Membros a tomar as medidas necessárias para assegurar a disponibilidade das redes públicas em caso de corte da rede devida a catástrofe natural [Directiva Interconexão 97/33/CE [1] e Directiva Telefonia Vocal 98/10/CE [2]]. Porém, o Comité sugere à Comissão que promova um estudo comparativo das medidas tomadas e da sua eficácia em todos os Estados-Membros.

3.2.1.2.2. As falsas declarações de pessoas singulares ou colectivas podem causar prejuízos, sendo necessário, para todas as transacções importantes, autenticar a identidade das pessoas e assegurar a veracidade das declarações.

3.2.1.2.3. Os protocolos SSL e IPsec permitem comunicar na Internet e em canais abertos com um certo nível de segurança, mas não oferecem garantia suficiente. A directiva sobre assinaturas electrónicas [3] prevê que um terceiro, o «prestador de serviços de certificação», possa oferecer tal garantia.

3.2.1.2.4. A adopção desta solução confronta-se, como a cifragem, com o problema da necessidade de interoperabilidade e de gestão das chaves. Numa VPN (rede virtual privada) é possível recorrer a soluções próprias, mas nas redes públicas é um dos grandes obstáculos.

3.2.1.2.5. Assim, a directiva sobre as assinaturas electrónicas constitui a base jurídica e o instrumento essencial para facilitar a autenticação electrónica na UE.

3.2.1.3. Novos desafios, novos riscos e análise custo-benefício

3.2.1.3.1. O Comité concorda com a análise dos novos desafios e riscos associados ao desenvolvimento rápido das tecnologias, à multiplicação e diversificação de terminais de acesso e aos perigos acrescidos de pirataria, com a generalização de terminais ligados permanentemente e com um endereço fixo. O Comité apoia a abordagem que pretende conciliar segurança e liberdade, protecção das redes e protecção da vida privada e da confidencialidade.

3.2.1.3.2. Além disso, se os meios de cifragem mais seguros exigiram uma evolução das legislações para permitir a «cifragem robusta», por vezes, por razões de segurança, esta foi demasiado tardia; porém, a dissimulação das mensagens no «ruído» de ficheiros de imagens ou som (esteganografia) permitia já às pessoas que desejassem contornar a lei sem serem detectadas dissimular o envio de uma mensagem cifrada.

3.2.1.3.3. Diversos algoritmos são utilizados e estão já disponíveis outros mais sofisticados, o que coloca sérios problemas de gestão de mensagens cifradas por diversos correspondentes utilizando métodos diferentes. Mesmo a recomendação de um sistema europeu, embora possa facilitar a comunicação no mercado interno, enfrentará a diversidade dos sistemas vigentes no resto do mundo, o que se repercute no custo da segurança e da sua gestão, ainda que certos sistemas eficazes estejam no domínio público e sejam gratuitos.

3.2.1.3.4. Contudo, o custo da não-segurança, num momento em que circulam dados cada vez mais sensíveis, é ainda maior. Em certa medida, a segurança integrar-se-á cada vez mais nos produtos.

3.2.1.3.5. O Comité acolhe favoravelmente a abordagem europeia proposta pela Comissão — embora esteja consciente dos seus limites — e reconhece a necessidade de uma acção pública para suprir as carências actuais do mercado, dada a importância dos interesses em jogo.

3.2.1.3.6. Existem já garantias jurídicas nas directivas da UE sobre a protecção de dados e no quadro regulamentar das telecomunicações. Contudo, estas medidas devem ser aplicadas num ambiente em evolução rápida, no domínio das tecnologias, da concorrência, da convergência das redes e da globalização, num momento em que o mercado tende a não investir suficientemente em segurança pelas razões descritas na comunicação, mesmo que o mercado da segurança esteja em rápida expansão no mundo.

---

[1] JO L 199 de 26.7.1997.
[2] JO L 101 de 1.4.1998.
[3] Directiva 1999/93/CE, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas electrónicas, JO L 13 de 19.1.2000, p. 12.

3.2.1.3.7. Como afirma a Comissão, é verdade que o mercado da segurança não é ainda perfeito. O investimento em segurança apenas é rentável se um número suficiente de pessoas adoptar a mesma abordagem. A busca de soluções deve pois passar pela cooperação. Na medida em que uma infinidade de produtos e serviços continua a utilizar soluções de propriedade, é necessário encorajar a investigação com vista à definição de normas com aceitação mais generalizada e mais seguras e à interoperabilidade dos sistemas de segurança. Entende o Comité que mais vale encorajar a fixação de critérios comuns a nível internacional do que sistemas de certificação--autenticação que podem penalizar o consumidor final.

3.2.1.3.8. Em primeiro lugar, devem ser aplicadas eficazmente as disposições jurídicas existentes a nível da UE. O quadro jurídico deve ser pertinente e eficaz e deve, portanto, evoluir continuamente.

3.2.1.3.9. Em segundo lugar, as forças do mercado não permitem actualmente gerar um nível de investimento suficiente nas tecnologias e nas práticas de segurança. As medidas políticas propostas pela Comissão podem reforçar o processo do mercado, que aliás começa a evoluir.

3.2.1.3.10. Por fim, os serviços de comunicação e informação são transfronteiriços. Por isso é necessária uma abordagem política europeia para assegurar o mercado interno destes serviços, beneficiar de soluções comuns e agir mais eficazmente a nível mundial.

3.2.1.3.11. O Comité está de acordo com a ideia de que os investimentos em melhor segurança das redes geram custos e benefícios sociais que não são correctamente reflectidos nos preços do mercado. No que respeita aos custos, os actores do mercado não são actualmente obrigados a assumir todas as responsabilidades resultantes do seu comportamento em matéria de segurança. O Comité considera que esta situação não se pode manter.

3.2.1.3.12. O Comité concorda também com a análise segundo a qual os benefícios da segurança também não se repercutem inteiramente nos preços de mercado, embora os investimentos dos operadores, fornecedores ou prestadores de serviços neste domínio beneficiam não apenas os seus clientes mas também toda a economia e a segurança geral das comunicações.

3.2.1.3.13. O Comité concorda também com a ideia de que os utilizadores não têm consciência de todos os riscos de segurança, ao mesmo tempo que grande número de operadores, vendedores ou prestadores de serviços têm dificuldade em avaliar a existência e amplitude das vulnerabilidades. De igual modo, numerosos serviços, aplicações e programas novos oferecem características atraentes que podem, porém, originar novas vulnerabilidades. Conviria testar mais rigorosamente os produtos antes da sua comercialização.

3.2.2. Observações na especialidade sobre o quadro político europeu proposto

3.2.2.1. O Comité está consciente da vulnerabilidade intrínseca da rede mundial, em particular no encaminhamento de pacotes de dados, dado que a crescente massa de dados em circulação não permite encarar a sua segurança geral por filtragem, fora dos terminais. O Comité apoia, na generalidade, as propostas de acção contidas no quadro político proposto.

3.2.3. Sensibilização

3.2.3.1. As propostas para sensibilizar todas as pessoas e organizações interessadas são razoáveis. A segurança dos terminais e das comunicações depende principalmente da sensibilização e acção informada dos próprios utilizadores.

3.2.4. Sistema europeu de informação rápida

3.2.4.1. O Comité apoia a proposta de um sistema europeu de alerta e informação rápida que indique os problemas e soluções a aplicar, bem como as outras propostas da Comissão na matéria em análise: detecção precoce, difusão de informação e de conselhos e cooperação europeia e mundial, desenvolvendo simultaneamente infra-estruturas adaptadas na União Europeia e a cooperação permanente e efectiva.

3.2.4.2. Contudo, no que respeita aos relatórios que as empresas deveriam elaborar, mas também, no entender do Comité, as administrações e outros organismos, o Comité compreende que o carácter confidencial do mecanismo de comunicação de ataques favorecerá o retorno de informação, mas lembra que há sempre fugas ou revelações públicas feitas por *hackers* e, assim, o conhecimento rápido da natureza dos ataques e falhas e, sobretudo, das medidas tomadas para os remediar constituiria antes um factor de confiança do público.

3.2.4.3. Na opinião do Comité, os sistemas de detecção e alerta devem também abranger a descoberta de falhas nos programas informáticos comerciais ou gratuitos e qualquer factor tecnológico ou outro que possa abrir a porta a eventuais ataques. O sistema de análise precoce poderá ter essa função, bem como a de controlo tecnológico e acompanhamento dos sítios dos *hackers* e piratas informáticos e de diversas publicações *underground* que tratam dos métodos disponíveis, nomeadamente publicando programas «chave na mão» de criação de vírus ou intrusão de que se servem os *script kiddies* ([1]).

3.2.5. Apoio tecnológico

3.2.5.1. O Comité aprova o previsto apoio aos esforços de investigação. Lembra porém que a cifragem é uma ciência dominada apenas por algumas dezenas de peritos no mundo, muitos dos quais trabalham para a NSA. Como reter os peritos europeus necessários para desenvolver a investigação? Que meios seriam eficazes na Europa? A NSA ([2]) tem 10 ou 15 anos de avanço e dispõe de meios de cálculo (e de descodificação) que parece difícil igualar rapidamente. Que meios concretos — e, necessariamente, de envergadura — serão postos ao serviço da investigação ([3])?

3.2.5.2. Uma política de integração de *hackers* e peritos «informais» existentes poderia ser uma pista complementar, em vez da atitude de rejeição, com marginalização ou penalização excessiva por confusão com actos muito graves, que parece desenvolver-se na Europa relativamente a pessoas que não causam qualquer dano aos outros ou à sociedade. Embora assegurando a penalização dissuasora dos actos de pirataria ou de terrorismo nas redes, haverá que não equiparar sistematicamente a estes actos as pesquisas de falhas de segurança efectuadas com uma finalidade de informação dos autores de programas ou dos gestores das redes com vista ao reforço da sua protecção, desde que tais pesquisas não sejam realizadas com intenção de causar danos, como em casos de sabotagem, desvio de dados confidenciais, utilização secreta da rede, enriquecimento pessoal ou difusão de vírus informáticos.

3.2.5.3. Tornar públicas descobertas sem que os interessados directos sejam informados com antecedência suficiente e sem o seu acordo constitui, no entanto, um acto repreensível que pode justificar um procedimento judicial proporcionado. Mas às pessoas que não cometam crimes ou delitos graves, nem causem danos pecuniários, conviria procurar integrá-las no quadro da legalidade e tirar proveito das suas competências, para bem da sociedade. Deste modo, estas competências não estariam expostas — por serem objecto de marginalização e criminalização — a serem desviadas ou utilizadas por criminosos ou terroristas.

3.2.6. Apoio a uma normalização e a uma certificação orientadas para as necessidades do mercado

3.2.6.1. O Comité concorda com a análise da Comissão sobre o excessivo número de normas e sistemas existentes, que dificultam a segurança e o progresso da assinatura e dos meios de pagamento electrónicos seguros e sublinha a necessidade de normas comuns, de critérios comuns, que permitam evitar a rigidez do mercado, e de interoperabilidade.

3.2.6.2. O Comité apoia as acções propostas, mas sublinha certas dificuldades associadas à natureza privada e insuficientemente representativa do «governo» actual da Internet que, nomeadamente, define as normas. É trabalho de grande fôlego que exige paciência e cooperação.

3.2.7. Quadro jurídico

3.2.7.1. O Comité aprova o projecto de especificações para as redes e a Internet no quadro legislativo existente em matéria de telecomunicações e protecção de dados.

3.2.7.2. O Comité considera que as acções propostas são razoáveis e aprova as iniciativas previstas para harmonizar o direito penal e reforçar entre os Estados-Membros a cooperação penal contra a cibercriminalidade, sem pôr em causa a liberalização do comércio dos instrumentos de cifragem robusta, os únicos capazes de assegurar segurança eficaz. A cooperação em matéria civil e comercial tem também um papel importante na luta contra os cibercriminosos (circuitos financeiros, fraude fiscal, etc.).

([1]) Jovens aprendizes de piratas, sem qualificações técnicas, que se contentam em copiar o que encontram nos sítios e publicações *underground*.

([2]) National Security Agency, Agência Nacional de Segurança dos Estados Unidos.

([3]) Parecer do CES sobre o Programa-quadro de IDT (JO C 260 de 17.9.2001, p. 3).

3.2.7.3. Contudo, na opinião do Comité, a cooperação penal deveria alargar-se ao plano global e a estratégia europeia neste domínio deveria ser objecto de uma linha de acção no quadro político proposto. O Comité nota com satisfação que será apresentada nas próximas semanas uma proposta formal da Comissão sobre esta matéria.

3.2.8. Segurança nas administrações públicas

3.2.8.1. O Comité aprova as acções previstas, tendo em conta o carácter pessoal de um grande número de dados tratados pelas administrações públicas e também porque os seus sítios podem ser objecto de ataques de tipo terrorista ou por razões de política interna ou externa do Estado, como o mostraram recentemente o *code red* (um vírus polimorfo) ou o «nimda». A Comissão deveria considerar estes últimos motivos de ataques como mais uma razão para melhorar a segurança dos seus sítios e redes oficiais e os dos Estados-Membros.

3.2.9. Cooperação internacional

3.2.9.1. No entender do Comité, trata-se de um aspecto essencial mas delicado e difícil da política europeia de segurança das redes e das comunicações que coloca sérios problemas de solidariedade interna e de política externa e de segurança comum, bem como de gestão das redes interligadas e da Internet.

3.2.9.2. A proposta de acção neste domínio, que consiste em prosseguir e desenvolver a cooperação nas diversas instâncias internacionais sobre a fiabilidade das redes, é diplomaticamente formulada em termos anódinos.

3.2.9.3. Contudo, o Comité considera que conviria debater nas instâncias internacionais apropriadas e no âmbito do diálogo transatlântico as questões de segurança, de interoperabilidade das chaves e dos sistemas de cifragem, dos problemas de deficiências eventuais de certas normas técnicas que poderiam ser conhecidos mas não divulgados por uma das partes. Seria igualmente desejável cooperar estreitamente em matéria de circulação internacional de dados pessoais, de cooperação penal e civil contra a cibercriminalidade, ou seja, da efectiva segurança e gestão transparente e equilibrada da rede mundial, cuja importância estratégica é reconhecida como essencial para a vida e o bem-estar das nossas sociedades. A OCDE, que trabalha sobre questões de segurança das redes, constitui uma das instâncias pertinentes de cooperação internacional nesta matéria. É urgente alcançar resultados práticos a nível global.

3.2.9.4. O Comité apoia e considera muito importante a proposta da Comissão de constituir, a nível europeu, um fórum que reúna todos os actores interessados para debater o conjunto de problemas e propor soluções às instituições.

4. **Conclusões**

4.1. Existem soluções de programas e equipamentos informáticos bastante eficazes e em constante evolução, como as descritas na comunicação. Além disso, a integridade de um ficheiro pode ser também garantida pelo uso de um algoritmo digital único que indique que o ficheiro transmitido não foi modificado.

4.2. Contudo, o Comité entende que a sensibilização dos utilizadores, a informação e a formação constituem a chave de toda a estratégia de segurança, pois sem elas os meios e soluções disponíveis não serão correctamente utilizados. Elas reforçam também a confiança na fiabilidade global do sistema desde que todos tomem regularmente as precauções elementares e as empresas invistam o necessário na segurança dos seus sistemas.

4.3. Porém, o custo da segurança é muito elevado e a falta de interoperabilidade das soluções constitui um obstáculo importante para cuja superação os sistemas livres poderão contribuir, estimulando a concorrência e a emulação.

4.4. Se estes problemas não forem rapidamente resolvidos no quadro europeu e internacional — aliás, a Europa deve assumir um lugar efectivo no «governo» da Internet —, vão continuar a dificultar o desenvolvimento da e-Europa, do comércio electrónico e da gestão das empresas, dos serviços públicos e das administrações.

4.5. Em todo o caso, é indispensável para a segurança das redes, conseguir a aplicação generalizada de medidas de protecção e defesa eficazes e proporcionadas, quer se trate de soluções informáticas para os particulares (antivírus actualizados regularmente) ou soluções combinadas, mais ou menos consistentes, para os outros utilizadores (corta-fogos, vigilância das portas de comunicação externa, separação [DMZ ([1])], escudos e outras técnicas, programas e equipamento informáticos pertinentes).

([1]) DMZ: DeMilitarized Zone (zona desmilitarizada).

4.6. A dissuasão através de sanções penais apropriadas é da competência dos Estados-Membros, mas o Comité entende que cabe à Comissão propor um quadro global unificador para a abordagem penal comunitária e a cooperação judiciária internacional.

4.7. A comercialização de certos produtos que podem ter «portas de acesso ocultas» (*backdoors*) [1] intencionais, cuja detecção pode levar anos, deve ser tida em consideração e sancionada, tal como programas de espionagem (*spyware*), frequentemente presentes nos programas de demonstração, em alguns programas gratuitos e em certos sistemas de registo de licenças em linha.

4.8. Mesmo as falhas eventualmente não intencionais levam tempo a ser corrigidas e podem ser utilizadas como *backdoors* por pessoas informadas.

[1] Portas de acesso ocultas.

4.9. Estes problemas de segurança deverão ser seguidos por autoridades nacionais *ad hoc*, independentes, imparciais e representativas, quer se trate de órgãos existentes, cuja competência haveria que alargar, ou de órgãos a criar onde ainda não existam (países candidatos, que será necessário associar), com vista a contribuir para formular recomendações e normas e proteger os direitos fundamentais. Com efeito, os projectos de legislação em preparação requerem um exame mais atento a fim de conciliar os imperativos da luta anti-terrorista com os princípios de liberdade individual, que devem ser preservados.

4.10. Na opinião do CES, a Internet deve sempre permanecer flexível e facilmente acessível e continuar a proporcionar um espaço de liberdade de informação e de comunicação numa sociedade aberta e democrática, tornando-se ao mesmo tempo mais segura para os utilizadores, no respeito da diversidade dos usos legais das redes e da Internet e da sua expansão.

Bruxelas, 28 de Novembro de 2001.

O Presidente

do Comité Económico e Social

Göke FRERICHS