Parecer do Comité das Regiões 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 107/27)

O COMITÉ DAS REGIÕES,

Tendo em conta 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» (COM(2001) 298 final);

Tendo em conta a decisão da Comissão, de 7 de Junho de 2001, de o consultar, em conformidade com o artigo 265.º, primeiro parágrafo, do Tratado que institui a Comunidade Europeia;

Tendo em conta a decisão do seu Presidente, de 2 de Julho de 2001, de atribuir a elaboração do parecer à Comissão 3 «Redes Transeuropeias, Transportes e Sociedade da Informação»;

Tendo em conta a decisão do seu Presidente, de 26 de Outubro de 2001, de designar Adela María Barrero Flórez relatora-geral encarregada da elaboração de parecer nesta matéria de harmonia com o artigo 40.º, n.º 2, do Regimento do Comité das Regiões;

Tendo em conta o 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: eEurope 2002» (COM(2000) 890 final — CdR 88/2001 fin);

Tendo em conta a «Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões — Garantir a segurança e a confiança nas comunicações electrónicas — Contribuição para a definição de um quadro europeu para as assinaturas digitais e a cifragem» (COM(97) 503 final);

Tendo em conta a «Comunicação da Comissão ao Conselho e ao Parlamento Europeu — eEurope 2002: Impacto e prioridades — Comunicação ao Conselho Europeu da Primavera, em Estocolmo, de 23 a 24 de Março de 2001» (COM(2001) 140 final);

Tendo em conta «eEurope 2002 — Uma sociedade da informação para todos: Projecto de plano de acção» (COM(2000) 330 final);

Tendo em conta o projecto de convenção do Conselho da Europa sobre cibercriminalidade (COM(2001) 103);

Tendo em conta a recomendação do Conselho, de 7 de Abril de 1995, relativa a critérios comuns de avaliação da segurança nas tecnologias da informação ([1]);

Tendo em conta a recomendação do Conselho, de 25 de Junho de 2001, relativa a um serviço de 24 horas por dia de combate ao crime de alta tecnologia ([2]);

Tendo em conta o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados ([3]);

Tendo em conta a Resolução n.º 9194/01 do Conselho, de 20 de Junho de 2001, sobre as necessidades operacionais das autoridades competentes em matéria de redes e serviços públicos de telecomunicações;

Tendo em conta as conclusões da Presidência do Conselho Europeu de Estocolmo de Março de 2001;

Tendo em conta a Directiva 90/388/CEE da Comissão, de 28 de Junho de 1990, relativa à concorrência nos mercados de serviços de telecomunicações;

([1]) JO L 93 de 26.4.1995.
([2]) JO C 187 de 3.7.2001.
([3]) JO L 8 de 12.1.2001.

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

Tendo em conta a Directiva 97/33/CE do Parlamento Europeu e do Conselho, de 30 de Junho de 1997, relativa à interligação no sector das telecomunicações com o objectivo de assegurar o serviço universal e a interoperabilidade através da aplicação dos princípios da oferta de rede aberta (ORA);

Tendo em conta a Directiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas;

Tendo em conta a Directiva 98/10/CE do Parlamento Europeu e do Conselho, de 26 de Fevereiro de 1998, relativa à aplicação da oferta de rede aberta (ORA) à telefonia vocal e ao serviço universal de telecomunicações num ambiente concorrencial;

Tendo em conta a Directiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas electrónicas;

Tendo em conta a Directiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre o comércio electrónico»);

Tendo em conta a proposta de directiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas [1];

Tendo em conta o projecto de parecer (CdR 257/2001 rev.), elaborado pela relatora-geral Adela María Barrero-Flórez (E/PSE), Directora-Geral dos Assuntos Europeus, Principado de Astúrias;

Considerando que as redes e os sistemas de informação se converteram num factor essencial do desenvolvimento social e económico da sociedade actual e que o seu adequado funcionamento é fundamental para as infra-estruturas vitais, tais como a energética e a viária, bem como para a maioria dos serviços públicos e privados e a economia em geral;

Considerando que a segurança das redes e dos sistemas de informação se converteu num requisito prévio para futuros progressos em novos serviços, novas fontes de riqueza económica, relações comerciais inovadoras, etc.;

Considerando o grave prejuízo que o crescente número de violações da segurança produz na confiança dos utilizadores das redes de informação;

Considerando que a falta de confiança nas redes e nos sistemas de informação produz um enfraquecimento na extensão generalizada dos novos serviços relacionados com a sociedade da informação e do conhecimento;

Considerando que a segurança destas redes e sistemas se converteu num repto essencial para os responsáveis políticos que precisam de aquilatar a sua importância, compreender os seus aspectos, os problemas de segurança em jogo e o papel que podem desempenhar na sua melhoria;

Considerando que, embora tenha sido criado um conjunto substancial de diplomas no âmbito das telecomunicações e da legislação para a protecção dos dados a nível nacional e comunitário, não foram adoptadas medidas específicas em matéria de segurança;

Considerando que muitos riscos de segurança das redes e dos sistemas de informação permanecem sem solução e noutros casos as soluções surgem lentamente no mercado, fruto de certas imperfeições deste;

Considerando que as administrações públicas têm um papel a desempenhar na solução das carências ou deficiências dos mercados;

---

[1] JO C 365 de 19.12.2000.

Considerando que a adopção de medidas políticas específicas para colmatar estas imperfeições pode reforçar o processo do mercado e, simultaneamente, melhorar o funcionamento do quadro jurídico;

Considerando que tais medidas devem integrar uma abordagem europeia para garantir o desenvolvimento da sociedade da informação e do conhecimento na UE, proporcionar os benefícios de soluções comuns e permitir uma acção efectiva a nível mundial;

Considerando que a complexidade do problema requer que sejam considerados os seus aspectos políticos, económicos, organizativos e técnicos, bem como o seu carácter descentralizado e global;

Considerando que os efeitos da falta de segurança nas redes e sistemas de informação das regiões europeias menos desenvolvidas podem agravar o fenómeno da fractura digital actualmente existente entre estas regiões e as mais desenvolvidas e seguras;

Considerando que os órgãos de poder regional e local podem e devem desempenhar um papel essencial na execução de uma política europeia de segurança das redes e dos sistemas de informação, dado que a proximidade dos cidadãos, organizações e empresas lhes oferece a necessária eficácia e idoneidade na aplicação das medidas concretas que sejam decididas,

aprovou na 41.ª reunião plenária de 14 e 15 de Novembro de 2001 (sessão de 15 de Novembro), por unanimidade o presente parecer.

Introdução

O Comité das Regiões

1. Compartilha com a Comissão a crescente preocupação que suscita a segurança das redes e dos sistemas de informação e a importância crítica que reveste não só para o desenvolvimento da sociedade da informação e do conhecimento, mas também para o actual sistema económico à escala mundial.

2. Concorda com a comunicação quanto à prioridade política que a União Europeia deve atribuir à segurança das redes e dos sistemas de informação. O mercado não foi capaz de dar uma resposta única porque existem muitas tecnologias e normas de segurança, mas carece de uma norma aberta e consensual.

3. Adere ao objectivo da comunicação de determinar em que esferas é necessário introduzir ou reforçar a intervenção pública a nível europeu ou nacional com o fim de decidir uma política comunitária sobre segurança das redes e dos sistemas de informação.

4. Mostra-se preocupado com o respeito das liberdades e direitos civis reconhecidos na Declaração Universal dos Direitos do Homem, no Pacto Internacional sobre os Direitos Civis e Políticos e na Convenção Europeia dos Direitos do Homem quanto às medidas a adoptar para aumentar a segurança das redes e sistemas de informação. Neste contexto, solicita o estabelecimento de limites claros para os poderes e competências que envolvam situações em que as liberdades civis fiquem comprometidas. O Comité das Regiões considera possível o equilíbrio entre o respeito das liberdades e direitos civis e a segurança das redes e sistemas de informação.

5. Duvida que esta política concertada a nível comunitário logre os objectivos de segurança perseguidos sem o acordo das organizações internacionais e das demais potências mundiais, dado o carácter transfronteiriço do problema.

6. Insta a Comissão a que, de acordo com a importância e a urgência de conferir a necessária segurança às redes e aos sistemas de informação, acelere a aplicação das medidas concretas aprovadas, dotando-as de suficientes recursos económicos.

Análise das questões associadas à segurança das redes e da informação

O Comité das Regiões

7. Considera pouco clara a definição de segurança das redes e da informação incluída na comunicação como «a capacidade de uma rede ou sistema da informação para resistir, com um dado nível de confiança, a eventos acidentais ou acções maliciosas que comprometem a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessa rede ou sistema» quando se refere a «nível de confiança». O Comité entende que as acções maliciosas ou intrusões numa rede ou sistema de informação não são aceitáveis, independentemente do «nível de confiança».

8. Considera muito preocupante que o investimento na segurança não seja prioritário nem proporcional para a generalidade dos operadores de serviços de telecomunicações e dos fornecedores de serviços de acesso que operam na Europa. Além disso, a existência de pequenos operadores regionais, cuja prioridade é alcançar uma posição no mercado que lhes permita obter resultados económicos positivos, o que lhes faz descuidar a segurança, é uma dificuldade e um factor a ter em consideração.

9. Crê que a confiança nos produtos de cifragem virá, em larga medida, da existência de requisitos e normas internacionais abertas e considera infrutíferas as iniciativas descoordenadas de alguns Estados-Membros para apoiar *software* de fonte aberta para cifragem, face à forte e indomável iniciativa de negócio do sector privado.

10. Concorda com a comunicação em que a concorrência entre os fornecedores de *software* não se traduz em maior investimento em matéria de segurança, impondo-se propor o estudo de medidas que favoreçam tais investimentos.

11. Considera necessária a obrigatoriedade por parte dos operadores de serviços de telecomunicações e fornecedores de serviços de acesso de cumprir o nível mínimo de segurança que será fixado no plano comunitário.

Abordagem de uma política europeia

O Comité das Regiões

12. Considera que o desenvolvimento equilibrado da sociedade da informação e do conhecimento na União Europeia facilitará a coesão e a estruturação da Europa das regiões, sendo, para tanto, indispensável garantir a segurança das redes e dos sistemas de informação.

13. Convém com a comunicação da Comissão nos benefícios sociais que o investimento na melhoria da segurança das redes e dos sistemas de informação implica e não pode deixar de sublinhar o elevado custo social que a falta de investimento por parte de fabricantes, operadores e fornecedores de serviços representa para a sociedade e para a prosperidade.

14. Insta a Comissão a estudar a necessidade de estabelecer critérios e normas de segurança que todos os sistemas de informação considerados básicos (serviços de interesse público), ligados às redes de telecomunicações, bem como as próprias redes, deverão obrigatoriamente cumprir.

15. Entende ser necessário aumentar ao máximo a segurança sem comprometer, porém, a facilidade e a qualidade do acesso em que se escora a sociedade da informação e do conhecimento, mas considera indispensável manter um nível mínimo de segurança, ainda que penalizando a qualidade do acesso.

16. Adere à comunicação da Comissão quanto:

— à necessidade comum de compreender as questões latentes associadas à segurança e as medidas específicas a adoptar,

— ao facto de as medidas políticas poderem reforçar o processo no mercado e, simultaneamente, melhorar o funcionamento do quadro jurídico,

— à necessidade de abordar uma política europeia para garantir o mercado interno destes serviços, proporcionar os benefícios de soluções comuns e permitir uma acção efectiva a nível mundial.

17. É partidário do complemento das acções de sensibilização propostas na comunicação com acções de apoio ou ajuda ao investimento em medidas de segurança para que o custo económico não venha a diferir a adopção de medidas que tenham sido reconhecidas necessárias.

18. Ressalta a importância de que, por razões de ordem operacional e prática, as administrações regionais e locais desempenhem um papel relevante em toda a campanha de sensibilização que seja organizada neste campo.

19. Compartilha com a comunicação a necessidade de fortalecer, urgentemente, o sistema CERT na União Europeia e de dotar os centros existentes de recursos humanos, técnicos e económicos suficientes.

20. Recomenda uma relação mais estreita, directa e activa dos CERT europeus com os potenciais beneficiários finais.

21. Aprova as acções propostas na comunicação quanto a um sistema europeu de alerta e informação sugerindo, ao mesmo tempo, a adopção de uma posição proactiva, como seja a criação de uma Agência Europeia de Segurança das Redes e dos Sistemas de Informação, que seja responsável, entre outras coisas, pela análise e ensaio de todo o *software* (sistemas operativos, navegadores, gestores de correio electrónico, etc.) destinado a ser utilizado em redes de informação públicas com o objectivo de identificar as «brechas» em matéria de segurança existentes no *software* que não é comercializado na União Europeia. O Comité das Regiões considera que o futuro Instituto de Protecção e Segurança do Cidadão (IPSC), dependente do Centro Comum de Investigação (CCI), não equivale, em natureza e missão, à Agência proposta.

22. O Comité das Regiões teme que toda a investigação sobre segurança das redes e da informação financiada pelos programas-quadro de investigação e desenvolvimento da UE que não seja apoiada pelos principais fabricantes de *software* do mercado não venha a obter o resultado prático almejado. O Comité propõe que se realize, independentemente, um esforço no sentido de obter dos principais fabricantes mundiais de *software* um maior compromisso com a investigação na segurança das redes e da informação e com a sua aplicação prática imediata.

23. Manifesta a sua preocupação quanto à actual inexistência de interoperabilidade entre as várias soluções tecnológicas dos fabricantes e ao seu desinteresse por elaborar normas comuns abertas.

24. Recomenda que não se fomente a utilização de determinadas soluções ou produtos de cifragem quando o caminho a seguir é a convergência de todas as soluções para uma norma comum aberta e aceite por todos os fabricantes.

25. Considera fundamental o estabelecimento de acordos entre os diferentes prestadores de serviços de certificação europeus sobre o reconhecimento mútuo dos respectivos certificados. Sem este acordo a utilidade dos certificados electrónicos será assaz limitada e, assim, a sua utilização atingirá níveis inferiores aos desejados. É motivo de preocupação a designação como prestadores de serviços de certificação de autoridades regionais com soluções tecnológicas não interoperáveis, o que complica, sem sombra de dúvida, o objectivo de uma Europa das Regiões coesa e estruturada.

26. Acolhe muito favoravelmente as iniciativas europeias na área da normalização das assinaturas electrónicas (EESSI), dos cartões inteligentes do programa eEuropa e da infra-estrutura de chaves públicas (PKI).

27. Concorda que a harmonização das especificações implicará uma maior interoperabilidade, permitindo simultaneamente aplicações mais expeditas por parte dos intervenientes no mercado.

28. Subscreve todas as acções propostas de apoio à normalização e certificação orientadas para o mercado e considera necessária a adopção de uma iniciativa no plano jurídico sobre o reconhecimento mútuo de certificados.

29. Considera oportuno comprovar periodicamente o grau de cumprimento por parte dos operadores de serviços de telecomunicações das medidas técnicas e organizativas que são obrigados a adoptar para salvaguardar a segurança dos seus serviços, nos termos do artigo 4.º da directiva relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

30. Deseja chamar a atenção da Comissão para a gravidade das consequências que a cibercriminalidade cometida por grupos terroristas pode ocasionar, já que não persegue outro objectivo que não seja o de causar o máximo dano possível a interesses colectivos como forma de chantagem política.

31. Subscreve todas as acções propostas no quadro jurídico e considera necessário aproximar e harmonizar as leis nacionais sobre cibercriminalidade para evitar a existência de Estados europeus onde se possa actuar impunemente ou incorrer em sanções penais menos rigorosas.

32. Propõe que se fomente a criação à escala nacional de unidades policiais especializadas em cibercriminalidade, onde elas não existam, e a coordenação de todas as existentes. Considera necessário, além disso, que sejam dotadas de recursos humanos e técnicos suficientes.

33. Aconselha a nomeação, em todos os Estados-Membros, de fiscais especiais contra a cibercriminalidade munidos de formação específica que lhes permita o exercício da acusação pública com a eficácia indispensável. A comunicação e a coordenação entre estes fiscais especiais devem ser consideradas fundamentais, bem como a formação especializada de juízes e magistrados que lhes permita arbitrar as questões submetidas a juízo respeitantes a actos judiciários em matéria de segurança das redes e dos que a elas acedem.

34. Concorda plenamente com a comunicação da Comissão Europeia em que o desenvolvimento da administração em linha, no qual muitos órgãos de poder regional e local apostaram com o fim de melhorar as relações com os cidadãos, a qualidade dos serviços que prestam e, em geral, o bem-estar e a participação democrática, faz das administrações públicas tanto potenciais modelos de demonstração de soluções seguras e eficazes como intervenientes no mercado capazes de influenciar a evolução neste domínio através das suas decisões de aquisições. Neste contexto, as administrações públicas têm o dever de servir de força motora ao desenvolvimento da sociedade da informação e do conhecimento, segundo as suas competências. Sem segurança nas redes e nos sistemas de informação que as administrações utilizam não haverá confiança por parte do cidadão e o dano causado ao desenvolvimento da nova sociedade será elevado.

35. Propõe que as acções relacionadas com as administrações públicas tenham como destinatários os três escalões da administração (local, regional e estatal) e que a interoperabilidade das soluções aplicadas seja um objectivo incontornável.

36. Apoia firmemente o reforço do diálogo com as organizações internacionais e parceiros em matéria de segurança das redes, em particular sobre o aumento da segurança de funcionamento nas redes electrónicas, e insta a Comissão a apreciar a celebração de uma cimeira mundial sobre a segurança das redes e dos sistemas de informação com a participação de fabricantes e operadores, bem como a criação de um Fórum Europeu da Cibercriminalidade. Convida ainda os Estados-Membros a ratificar a Convenção do Conselho da Europa sobre Cibercriminalidade, recentemente aprovada, de molde a permitir a sua entrada em vigor e a agilizar os instrumentos normativos nela incorporados.

Bruxelas, 15 de Novembro de 2001.

O Presidente

do Comité das Regiões

Jos CHABERT