

Proposta de decisão-quadro do Conselho relativa a ataques contra os sistemas de informação

(2002/C 203 E/16)

COM(2002) 173 final — 2002/0086(CNS)

(Apresentada pela Comissão em 19 de Abril de 2002)

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia e, nomeadamente, o seu artigo 29.º, o n.º 1, alínea a), do seu artigo 30.º, o seu artigo 31.º e o n.º 2, alínea b), do seu artigo 34.º,

Tendo em conta a proposta da Comissão,

Tendo em conta o parecer do Parlamento Europeu,

Considerando o seguinte:

- (1) A prática de ataques contra os sistemas de informação é uma evidência, nomeadamente devido à ameaça que representa a criminalidade organizada, existindo uma crescente inquietação perante a eventualidade de ataques terroristas contra os sistemas de informação pertencentes à infra-estrutura vital dos Estados-Membros. Esta situação é susceptível de comprometer a realização de uma sociedade da informação mais segura e de um espaço de liberdade, de segurança e de justiça, e exige, portanto, uma resposta a nível da União Europeia.
- (2) Uma resposta eficaz a essas ameaças pressupõe uma abordagem global em matéria de segurança das redes e da informação, como foi sublinhado no Plano de Acção «Europa, na comunicação da Comissão intitulada «Segurança das redes e da informação: Proposta de abordagem de uma política europeia»⁽¹⁾ e na resolução do Conselho, de 6 de Dezembro de 2001, sobre uma abordagem comum e acções específicas no domínio da segurança das redes e da informação.
- (3) A necessidade de reforçar a sensibilização para os problemas associados à segurança da informação e fornecer assistência prática foi igualmente sublinhada pela resolução do Parlamento Europeu de 5 de Setembro de 2001⁽²⁾.

(4) As consideráveis lacunas jurídicas e diferenças entre as legislações dos Estados-Membros neste domínio prejudicam a luta contra a criminalidade organizada e o terrorismo e obstam a uma cooperação eficaz dos serviços policiais e judiciais no caso de ataques contra os sistemas de informação. A natureza transnacional e sem fronteiras das redes de telecomunicações electrónicas modernas revela que os ataques contra os sistemas de informação têm frequentemente uma dimensão internacional, evidenciando assim a necessidade urgente de prosseguir a aproximação dos direitos penais neste domínio.

(5) O Plano de Acção do Conselho e da Comissão sobre a melhor forma de aplicar as disposições do Tratado de Amsterdão relativas à criação de um espaço de liberdade, de segurança e de justiça⁽³⁾, o Conselho Europeu de Tampere, de 15 e 16 de Outubro de 1999, o Conselho Europeu de Santa Maria da Feira, de 19 e 20 de Junho de 2000, o Painel de Avaliação da Comissão⁽⁴⁾, e a resolução do Parlamento Europeu de 19 de Maio de 2000⁽⁵⁾, mencionam ou solicitam medidas legislativas contra a criminalidade que utiliza as tecnologias avançadas, nomeadamente definições, incriminações e sanções comuns.

(6) É necessário completar o trabalho realizado pelas organizações internacionais, especialmente a nível do Conselho da Europa sobre a aproximação do direito penal e os trabalhos do G8 sobre a cooperação transnacional no domínio da criminalidade que utiliza as tecnologias avançadas, propondo uma abordagem comum neste domínio a nível da União Europeia. Este pedido foi desenvolvido na comunicação que a Comissão dirigiu ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões intitulada, «Criar uma sociedade da informação mais segura reforçando a segurança das infra-estruturas da informação e lutando contra a cibercriminalidade»⁽⁶⁾.

(7) As normas de direito penal em matéria de ataques contra os sistemas de informação devem ser aproximadas, a fim de assegurar a melhor cooperação policial e judiciária possível no que diz respeito às infracções associadas a este tipo de ataques e contribuir para a luta contra a criminalidade organizada e o terrorismo.

⁽¹⁾ COM(2001) 298.

⁽²⁾ [2001/2098(INI)].

⁽³⁾ JO C 19 de 23.1.1999.

⁽⁴⁾ COM(2001) 278 final.

⁽⁵⁾ A5-0127/2000.

⁽⁶⁾ COM(2000) 890.

- (8) A decisão-quadro relativa ao mandado de captura europeu, o anexo à Convenção Europol e a decisão do Conselho que cria a Eurojust, compreendem referências à criminalidade informática que necessitam de ser definidas de forma mais rigorosa. Para efeitos desses instrumentos, a criminalidade informática deve ser entendida no sentido de abranger os ataques contra sistemas de informação tal como definidos na presente decisão-quadro, o que permitirá um maior grau de aproximação dos elementos constitutivos dessas infracções. A presente decisão-quadro completa igualmente a decisão-quadro relativa à luta contra o terrorismo, que abrange as infracções terroristas causadoras de destruição maciça de uma infra-estrutura, incluindo um sistema de informação, e susceptíveis de colocar em risco a vida de pessoas ou de causar importantes prejuízos económicos.
- (9) Todos os Estados-Membros ratificaram a Convenção do Conselho da Europa, de 28 de Janeiro de 1981, para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal. Os dados de carácter pessoal tratados no contexto da aplicação da presente decisão-quadro serão protegidos em conformidade com os princípios estabelecidos na referida convenção.
- (10) São indispensáveis definições comuns neste domínio, especialmente em relação aos sistemas de informação e aos dados informáticos, a fim de assegurar a aplicação coerente da presente decisão-quadro nos Estados-Membros.
- (11) É necessário adoptar uma abordagem comum para os elementos constitutivos das infracções penais, prevendo uma infracção comum por acesso ilícito a determinado sistema de informação e por interferência ilícita num sistema de informação.
- (12) É necessário evitar uma incriminação exagerada, nomeadamente para os comportamentos pouco graves ou insignificantes, bem como a incriminação dos titulares de direitos e das pessoas autorizadas, designadamente os utilizadores privados ou profissionais legítimos, os administradores, os verificadores e os operadores de redes e sistemas, os investigadores científicos reconhecidos e as pessoas autorizadas a testar um sistema, quer a pessoa trabalhe a nível da empresa ou seja recrutada no exterior e a quem seja dada autorização para testar a segurança de determinado sistema.
- (13) É necessário que os Estados-Membros estabeleçam sanções eficazes, proporcionadas e dissuasivas para reprimir os ataques contra os sistemas de informação, incluindo penas de prisão nos casos graves.
- (14) É necessário prever penas mais severas se determinadas circunstâncias associadas a um ataque contra determinado sistema de informação constituírem uma ameaça acrescida para a sociedade. Nestes casos, as sanções de que são passíveis os autores de infracções devem ser suficientes para que ataques contra os sistemas de informação sejam abrangidos pelo âmbito de aplicação dos instrumentos já adoptados para efeitos da luta contra a criminalidade organizada, nomeadamente a Acção Comum 98/733/JAI, de 21 de Dezembro de 1998, adoptada pelo Conselho com base no artigo K.3 do Tratado da União Europeia, relativa à incriminação da participação numa organização criminosa nos Estados-Membros da União Europeia ⁽¹⁾.
- (15) Devem ser tomadas medidas para que as pessoas colectivas possam ser responsabilizadas pelas infracções penais mencionadas no presente acto caso sejam praticadas em seu benefício, e para que cada Estado-Membro tenha competência relativamente a infracções praticadas contra sistemas de informação se o seu autor estiver fisicamente presente no seu território ou se o sistema de informação se encontrar no território deste Estado-Membro.
- (16) Devem ser igualmente previstas medidas de cooperação entre os Estados-Membros, a fim de assegurar uma acção eficaz contra os ataques visando os sistemas de informação. Devem ser designados pontos de contacto operacionais para o intercâmbio de informações.
- (17) Como os objectivos consistindo em garantir que ataques contra os sistemas de informação sejam puníveis, em todos os Estados-Membros, com sanções penais efectivas, proporcionadas e dissuasivas, e em melhorar e favorecer a cooperação judiciária suprimindo os obstáculos potenciais, não podem ser suficientemente realizados pelos Estados actuando unilateralmente, pois as normas devem ser comuns e compatíveis, e que os referidos objectivos podem pois ser melhor alcançados a nível da União, esta pode adoptar medidas, em conformidade com o princípio de subsidiariedade estabelecido no artigo 2.º do Tratado da UE e previsto no artigo 5.º do Tratado CE. Em conformidade com o princípio da proporcionalidade referido no último artigo, a presente decisão-quadro do Conselho é limitada ao estritamente necessário para alcançar esses objectivos.
- (18) A presente decisão-quadro não afecta as competências da Comunidade Europeia.
- (19) A presente decisão-quadro respeita os direitos fundamentais e os princípios reconhecidos, nomeadamente pela Carta dos Direitos Fundamentais da União Europeia, designadamente os seus capítulos II e VI,

APROVOU A PRESENTE DECISÃO-QUADRO:

Artigo 1.º

Âmbito de aplicação e objectivo da decisão-quadro

A presente decisão-quadro tem por objectivo reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados encarregues da aplicação da lei nos Estados-Membros, graças a uma aproximação das suas disposições penais no domínio dos ataques contra os sistemas de informação.

⁽¹⁾ JO L 351 de 29.12.1998, p. 1.

Artigo 2.º**Definições**

Para efeitos da presente decisão-quadro, entende-se por:

- a) «Rede de comunicações electrónicas», os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou de encaminhamento e outros meios que permitam o transporte de sinais por fio, por feixes hertzianos, por meios ópticos ou outros meios electromagnéticos, incluindo redes de satélite, redes terrestres fixas (comutação de circuitos e comutação de pacotes, incluindo a internet) e móveis, sistemas de electricidade por cabo, na medida em que sejam utilizados para transmissão de sinais, redes para difusão de rádio e televisão e redes de televisão por cabo, independentemente do tipo de informação transportada;
- b) «Computador», qualquer aparelho ou grupo de aparelhos interligados ou ligados entre si, um ou vários dos quais executam, graças a um programa, o tratamento automático de dados informáticos;
- c) «Dados informáticos», qualquer representação de factos, de informações ou de conceitos criados ou inseridos sob uma forma que permite o seu tratamento através de um sistema de informação, nomeadamente um programa susceptível de gerar um sistema de informação para executar uma função;
- d) «Sistema de informação», os computadores e as redes de comunicações electrónicas, bem como os dados informáticos armazenados, tratados, recuperados ou transmitidos por aqueles tendo em vista o seu funcionamento, utilização, protecção e manutenção;
- e) «Pessoa colectiva», a entidade à qual o direito em vigor reconhece esse estatuto, com excepção dos Estados e outras entidades públicas no exercício de prerrogativas de autoridade pública e das organizações internacionais de direito público;
- f) «Pessoa autorizada», a pessoa singular ou colectiva que tem o direito, por força de um contrato, de uma lei ou de uma autorização legal, de utilizar, de administrar, de controlar, de testar, de realizar investigações científicas legítimas ou de explorar de qualquer outra forma um sistema de informação, e que actua em conformidade com esse direito ou autorização;
- g) «Sem ter o direito», significa que os actos de pessoas autorizadas ou outros comportamentos cujo carácter lícito é reconhecido pelo direito nacional são excluídos.

Artigo 3.º**Acesso ilícito aos sistemas de informação**

Os Estados-Membros assegurarão que o acesso intencional, sem ter o direito, à totalidade ou parte de um sistema de informação seja punido como infracção penal se é praticado:

i) contra qualquer parte de um sistema de informação objecto de medidas de protecção específicas, ou

ii) com a intenção de causar danos a uma pessoa singular ou colectiva, ou

iii) com a intenção de obter um benefício económico

Artigo 4.º**Interferência ilícita nos sistemas de informação**

Os Estados-Membros assegurarão que os actos intencionais seguintes, sem ter o direito, sejam punidos como infracção penal:

- a) Perturbar ou interromper gravemente o funcionamento de um sistema de informação introduzindo, transmitindo, danificando, apagando, deteriorando, alterando, suprimindo ou tornando inacessíveis dados informáticos;
- b) Apagar, deteriorar, alterar, suprimir ou tornar inacessíveis dados informáticos de um sistema de informação quando foram praticados com a intenção de causar danos a uma pessoa singular ou colectiva.

Artigo 5.º**Instigação, ajuda, cumplicidade e tentativa**

1. Os Estados-Membros assegurarão que a instigação, a ajuda ou a cumplicidade intencionais de prática de alguma das infracções referidas nos artigos 3.º e 4.º sejam punidas como infracção penal.

2. Os Estados-Membros assegurarão que a tentativa de prática das infracções referidas nos artigos 3.º e 4.º seja punida como infracção penal.

Artigo 6.º**Sanções**

1. Os Estados-Membros assegurarão que as infracções referidas nos artigos 3.º, 4.º e 5.º sejam puníveis com penas efectivas, proporcionadas e dissuasivas, compreendendo penas privativas de liberdade cuja duração máxima não pode ser inferior a um ano nos casos graves. Devem ser excluídos dos casos graves os actos que não causaram danos ou não tiveram por resultado benefícios económicos.

2. Os Estados-Membros deverão prever a possibilidade de serem aplicadas multas em complemento ou substituição das penas privativas de liberdade.

*Artigo 7.º***Circunstâncias agravantes**

1. Os Estados-Membros assegurarão que as infracções referidas nos artigos 3.º, 4.º e 5.º sejam puníveis com uma pena privativa de liberdade, que não pode ser inferior a quatro anos, se forem praticadas de acordo com as seguintes circunstâncias:

- a) A infracção foi praticada no âmbito de uma organização criminosa, tal como definida na Acção Comum 98/733/JAI, de 21 de Dezembro de 1998, relativa à incriminação da participação numa organização criminosa nos Estados-Membros da União Europeia, independentemente da pena aí referida;
- b) A infracção causou ou teve por resultado importantes prejuízos económicos, directos ou indirectos, lesões corporais a uma pessoa singular ou danos consideráveis a parte de uma infra-estrutura vital do Estado-Membro em causa;
- c) A infracção teve por resultado lucros importantes.

2. Os Estados-Membros assegurarão que as infracções referidas nos artigos 3.º e 4.º sejam puníveis com uma pena privativa de liberdade superior às penas previstas ao abrigo do artigo 6.º, se o infractor tiver sido condenado por essa infracção mediante sentença transitada em julgado num dos Estados-Membros.

*Artigo 8.º***Circunstâncias especiais**

Não obstante o disposto nos artigos 6.º e 7.º, os Estados-Membros assegurarão que as penas mencionadas nestes últimos artigos possam ser reduzidas se a autoridade judiciária competente considerar que o autor da infracção apenas causou danos pouco significativos.

*Artigo 9.º***Responsabilidade das pessoas colectivas**

1. Os Estados-Membros assegurarão que as pessoas colectivas possam ser consideradas responsáveis pelos actos referidos nos artigos 3.º, 4.º e 5.º, praticados em seu benefício por qualquer pessoa que ocupe um cargo de dirigente, agindo individualmente ou integrando um órgão da pessoa colectiva, com base num dos seguintes elementos:

- a) Poderes de representação da pessoa colectiva;
- b) Autoridade para tomar decisões em nome da pessoa colectiva; ou

- c) Autoridade para exercer funções de controlo a nível da pessoa colectiva.

2. Para além dos casos previstos no n.º 1, os Estados-Membros assegurarão que uma pessoa colectiva possa ser considerada responsável quando a falta de vigilância ou de controlo, por parte da pessoa referida no n.º 1, tiver possibilitado a prática das infracções referidas nos artigos 3.º, 4.º e 5.º, em benefício dessa pessoa colectiva, por uma pessoa sob a sua autoridade.

3. A responsabilidade de uma pessoa colectiva nos termos do n.º 1 e n.º 2 não exclui o procedimento penal contra as pessoas singulares que praticarem as infracções ou os actos referidos nos artigos 3.º, 4.º e 5.º.

*Artigo 10.º***Sanções aplicáveis às pessoas colectivas**

1. Os Estados-Membros assegurarão que uma pessoa colectiva declarada responsável por força do n.º 1 do artigo 9.º seja passível de sanções efectivas, proporcionadas e dissuasivas, que deverão incluir multas de carácter penal ou não penal e eventualmente outras sanções, designadamente:

- a) Exclusão do benefício de vantagens ou ajudas públicas;
- b) Proibição temporária ou definitiva de exercer actividades comerciais;
- c) Sujeição a controlo judiciário; ou
- d) Medidas judiciais de dissolução.

2. Os Estados-Membros assegurarão que uma pessoa colectiva declarada responsável por força do n.º 2 do artigo 9.º seja passível de sanções ou medidas efectivas, proporcionadas e dissuasivas.

*Artigo 11.º***Competência**

1. Cada Estado-Membro determinará a sua competência relativamente às infracções referidas nos artigos 3.º, 4.º e 5.º, sempre que:

- a) A infracção tiver sido praticada em todo ou parte do seu território; ou

b) O seu autor seja um cidadão nacional, se o acto afectar indivíduos ou grupos desse Estado; ou

c) A infracção tiver sido praticada em benefício de uma pessoa colectiva cuja sede social se situe no território desse Estado-Membro.

2. Na determinação da sua competência em conformidade com a alínea a) do n.º 1, cada Estado-Membro assegurará que sejam incluídos os seguintes casos:

a) O autor da infracção praticou o acto quando se encontrava fisicamente presente no território desse Estado-Membro, independentemente de a infracção visar ou não um sistema de informação situado no seu território; ou

b) A infracção foi praticada contra um sistema de informação situado no território desse Estado-Membro, independentemente de o autor da infracção se encontrar ou não fisicamente presente no seu território.

3. Um Estado-Membro pode decidir que não aplicará, ou que aplicará apenas em casos ou circunstâncias especiais, a regra de competência estabelecida nas alíneas b) e c) do n.º 1.

4. Cada Estado-Membro tomará as medidas necessárias para estabelecer a sua competência em relação às infracções referidas nos artigos 3.º a 5.º, nos casos em que se recusar a entregar ou a extraditar um suspeito ou culpado da prática dessas infracções para outro Estado-Membro ou país terceiro.

5. Se mais de um Estado-Membro for competente pela apreciação de uma infracção e se qualquer um dos Estados-Membros interessados pode validamente proceder ao julgamento da causa com base nos mesmos factos, os Estados-Membros interessados cooperarão a fim de decidir qual destes será competente com o objectivo, se possível, de centralizar os processos num único Estado-Membro. Para este efeito, os Estados-Membros podem recorrer a qualquer entidade ou mecanismo estabelecido a nível da União Europeia visando facilitar a cooperação entre as suas autoridades judiciárias e a coordenação das suas acções.

6. Os Estados-Membros informarão do facto o Secretariado-Geral do Conselho e a Comissão se decidiram aplicar o disposto no n.º 3, indicando, se for caso disso, os casos ou as circunstâncias especiais em que a decisão é aplicável.

Artigo 12.º

Intercâmbio de informações

1. Para efeitos do intercâmbio de informações relativas às infracções referidas nos artigos 3.º, 4.º e 5.º, e em conformidade com as normas em matéria de protecção de dados, os Estados-Membros assegurarão a designação de pontos de contacto operacionais disponíveis 24 horas por dia e sete dias por semana.

2. Cada Estado-Membro informará o Secretariado-Geral do Conselho e a Comissão do nome do seu ponto de contacto designado tendo em vista o intercâmbio de informações sobre as infracções relacionadas com os ataques contra os sistemas de informação. O Secretariado-Geral notificará esta informação aos outros Estados-Membros.

Artigo 13.º

Execução

1. Os Estados-Membros tomarão as medidas necessárias para dar cumprimento à presente decisão-quadro até 31 de Dezembro de 2003.

2. Os Estados-Membros comunicarão ao Secretariado-Geral do Conselho e à Comissão, o texto das disposições de transposição para o seu direito nacional, bem como informações sobre qualquer outra medida que adoptem para dar cumprimento às obrigações que lhes são impostas pela presente decisão-quadro.

3. Com essa base, a Comissão apresentará, até 31 de Dezembro de 2004, um relatório ao Parlamento Europeu e ao Conselho sobre a aplicação da presente decisão-quadro, acompanhado, se necessário, de propostas legislativas.

4. O Conselho avaliará a medida em que os Estados-Membros cumpriram as obrigações impostas pela presente decisão-quadro.

Artigo 14.º

Entrada em vigor

A presente decisão-quadro entrará em vigor no vigésimo dia seguinte à sua publicação no *Jornal Oficial das Comunidades Europeias*.