(Actos adoptados em aplicação do título VI do Tratado da União Europeia)

DECISÃO-QUADRO 2005/222/JAI DO CONSELHO

de 24 de Fevereiro de 2005

relativa a ataques contra os sistemas de informação

O CONSELHO DA UNIÃO EUROPEIA,

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

Tendo em conta a proposta da Comissão,

Tendo em conta o parecer do Parlamento Europeu [1],

Considerando o seguinte:

(1) 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 responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação.

(2) Há provas de ataques contra os sistemas de informação, nomeadamente devido à ameaça que representa a criminalidade organizada, existindo uma crescente inquietação perante a eventualidade de ataques terroristas contra os sistemas de informação que constituem a infra-estrutura vital dos Estados-Membros. Esta ameaça poderá comprometer a instauração de uma sociedade da informação mais segura e de um espaço de liberdade, de segurança e de justiça, exigindo, portanto, uma resposta ao nível da União Europeia.

(3) 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 «*e*Europe», na Comunicação da Comissão intitulada «Segurança das redes e da informação: proposta de abordagem de uma política europeia» e na Resolução do Conselho de 28 de Janeiro de 2002, sobre uma abordagem comum e acções específicas no domínio da segurança das redes e da informação [2].

(4) A necessidade de reforçar a sensibilização para os problemas associados à segurança da informação e de fornecer assistência prática foi igualmente sublinhada pela Resolução do Parlamento Europeu de 5 de Setembro de 2001.

(5) As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros neste domínio podem entravar a luta contra a criminalidade organizada e o terrorismo e podem dificultar uma cooperação policial e judiciária eficaz no âmbito de ataques contra os sistemas de informação. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio.

(6) O Plano de Acção do Conselho e da Comissão sobre a melhor forma de aplicar as disposições do Tratado de Amesterdão 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 e a Resolução do Parlamento Europeu de 19 de Maio de 2000 mencionam ou requerem medidas legislativas contra a criminalidade de alta tecnologia, nomeadamente definições, incriminação e sanções comuns.

(7) É necessário completar o trabalho realizado pelas organizações internacionais, especialmente ao nível do Conselho da Europa, no domínio da aproximação do direito penal e os trabalhos do G8 sobre cooperação transnacional no âmbito da criminalidade de alta tecnologia, propondo uma abordagem comum neste domínio ao nível da União Europeia. Este pedido foi desenvolvido na Comunicação que a Comissão dirigiu ao Conselho, ao Parlamento Europeu, ao Comité Económico reforçando a segurança das infra-estruturas da informação e lutando contra a cibercriminalidade.

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

[1] JO C 300 E de 11.12.2003, p. 26.
[2] JO C 43 de 16.2.2002, p. 2.
[3] JO C 19 de 23.1.1999, p. 1.

(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) É importante estabelecer definições comuns neste domínio, especialmente em relação aos sistemas de informação e aos dados informáticos, a fim de assegurar uma abordagem coerente da aplicação da presente decisão-quadro nos Estados-Membros.

(11) É necessário adoptar uma abordagem comum para os elementos constitutivos das infracções penais, prevendo infracções comuns por acesso ilegal a determinado sistema de informação, por interferência ilegal no sistema e por interferência ilegal nos dados.

(12) No interesse do combate à criminalidade informática, cada Estado-Membro deverá assegurar uma cooperação judiciária eficaz no que diz respeito às infracções baseadas nos tipos de comportamento a que se referem os artigos 2.º, 3.º, 4.º e 5.º

(13) É necessário evitar uma incriminação exorbitante, nomeadamente de casos insignificantes, bem como a incriminação de titulares de direitos e de pessoas autorizadas.

(14) É necessário que os Estados-Membros estabeleçam sanções para combater os ataques contra os sistemas de informação. Essas sanções deverão ser efectivas, proporcionadas e dissuasivas.

(15) É adequado prever penas mais severas nos casos em que um ataque contra determinado sistema de informação tenha sido praticado no âmbito de uma organização criminosa, tal como definida na Acção Comum 98/733/JAI do Conselho, de 21 de Dezembro de 1998, relativa à incriminação da participação numa organização criminosa nos Estados-Membros da União Europeia [1]. É igualmente adequado prever penas mais severas quando um tal ataque tiver causado danos graves ou lesado interesses essenciais.

(16) Deverão ser igualmente adoptadas medidas de cooperação entre os Estados-Membros, a fim de assegurar uma acção eficaz contra os ataques que visem os sistemas de informação. Os Estados-Membros devem, pois, recorrer à actual rede de pontos de contacto operacionais referida na 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], para efeitos de troca de informações.

(17) Atendendo a que os objectivos da presente decisão-quadro, a saber, garantir que os ataques contra os sistemas de informação sejam puníveis em todos os Estados-Membros com sanções penais efectivas, proporcionadas e dissuasivas, bem como melhorar e favorecer a cooperação judiciária, suprimindo potenciais dificuldades, não podem ser suficientemente realizados pelos Estados-Membros, já que as normas devem ser comuns e compatíveis, e podem, pois, ser melhor alcançados ao nível da União, esta pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado CE. Em conformidade com o princípio da proporcionalidade consagrado neste mesmo artigo, a presente decisão-quadro não excede o necessário para alcançar aqueles objectivos.

(18) A presente decisão-quadro respeita os direitos fundamentais e os princípios reconhecidos pelo artigo 6.º do Tratado União Europeia e reflectidos na Carta dos Direitos Fundamentais da União Europeia, designadamente nos capítulos II e VI,

ADOPTOU A PRESENTE DECISÃO-QUADRO:

Artigo 1.º

Definições

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

a) «Sistema de informação», qualquer dispositivo ou qualquer grupo de dispositivos interligados ou associados, um ou vários dos quais executem, graças a um programa, o tratamento automático de dados informáticos, bem como dados informáticos por eles armazenados, tratados, recuperados ou transmitidos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;

b) «Dados informáticos», qualquer representação de factos, informações ou conceitos, de forma a serem processados num sistema de informação, nomeadamente um programa capaz de permitir que um sistema de informação execute uma dada função;

c) «Pessoa colectiva», qualquer entidade que beneficie desse estatuto por força do direito aplicável, com excepção do Estado ou de outras entidades de direito público no exercício das suas prerrogativas de autoridade pública e das organizações internacionais de direito público;

[1] JO L 351 de 29.12.1998, p. 1.

[2] JO C 187 de 3.7.2001, p. 5.

d) «Não autorizado», acesso ou interferência não consentidos pelo proprietário, por outro titular do direito do sistema ou de parte dele, ou não permitidos nos termos do direito nacional.

Artigo 2.º

Acesso ilegal aos sistemas de informação

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que o acesso intencional, não autorizado, à totalidade ou a parte de um sistema de informação seja punível como infracção penal, pelo menos nos casos que não sejam de menor gravidade.

2. Os Estados-Membros podem decidir que os comportamentos referidos no n.º 1 são puníveis apenas quando a infracção tiver sido cometida em violação de uma medida de segurança.

Artigo 3.º

Interferência ilegal no sistema

Cada Estado-Membro deve tomar as medidas necessárias para assegurar que o acto intencional e não autorizado de impedir ou interromper gravemente o funcionamento de um sistema de informação, introduzindo, transmitindo, danificando, apagando, deteriorando, alterando, suprimindo ou tornando inacessíveis os dados informáticos, seja punível como infracção penal, pelo menos nos casos que não sejam de menor gravidade.

Artigo 4.º

Interferência ilegal nos dados

Cada Estado-Membro deve tomar as medidas necessárias para assegurar que o acto intencional e não autorizado de apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis os dados informáticos de um sistema de informação seja punível como infracção penal, pelo menos nos casos que não sejam de menor gravidade.

Artigo 5.º

Instigação, auxílio, cumplicidade e tentativa

1. Cada Estado-Membro deve assegurar que a instigação, o auxílio e a cumplicidade na prática de alguma das infracções referidas nos artigos 2.º, 3.º e 4.º sejam puníveis como infracção penal.

2. Cada Estado-Membro deve assegurar que a tentativa de prática das infracções referidas nos artigos 2.º, 3.º e 4.º seja punível como infracção penal.

3. Cada Estado-Membro pode decidir não aplicar o n.º 2 relativamente às infracções referidas no artigo 2.º

Artigo 6.º

Sanções

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º sejam passíveis de sanções penais efectivas, proporcionadas e dissuasivas.

2. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 3.º e 4.º sejam passíveis de pena privativa de liberdade com duração máxima de, pelo menos, um a três anos.

Artigo 7.º

Circunstâncias agravantes

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que a infracção referida no n.º 2 do artigo 2.º e as referidas nos artigos 3.º e 4.º sejam passíveis de pena privativa de liberdade com duração máxima de, pelo menos, dois a cinco anos quando forem praticadas no âmbito de uma organização criminosa, tal como definida na Acção Comum 98/733/JAI, independentemente do nível da pena nesta referido.

2. Um Estado-Membro pode também tomar as medidas a que se refere o n.º 1 nos casos em que a infracção em causa tenha causado danos graves ou lesado interesses essenciais.

Artigo 8.º

Responsabilidade das pessoas colectivas

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis pelas infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º, praticadas em seu benefício por qualquer pessoa, agindo individualmente ou enquanto integrando um órgão da pessoa colectiva, que nela ocupe uma posição dominante baseada:

a) Nos seus poderes de representação da pessoa colectiva; ou

b) No seu poder para tomar decisões em nome da pessoa colectiva; ou

c) Na sua autoridade para exercer controlo dentro da pessoa colectiva.

2. Para além dos casos previstos no n.º 1, os Estados-Membros devem assegurar que uma pessoa colectiva possa ser considerada responsável sempre que a falta de vigilância ou de controlo por parte de uma pessoa referida no n.º 1 tenha tornado possível a prática, por uma pessoa que lhe esteja subordinada, das infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º, em benefício dessa pessoa colectiva.

3. A responsabilidade de uma pessoa colectiva nos termos dos n.os 1 e 2 não exclui a instauração de procedimento penal contra as pessoas singulares envolvidas na qualidade de autoras, instigadoras ou cúmplices nas infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º

Artigo 9.º

Sanções aplicáveis às pessoas colectivas

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do n.º 1 do artigo 8.º seja passível de sanções efectivas, proporcionadas e dissuasivas, incluindo multas ou coimas e eventualmente outras sanções, designadamente:

a) Exclusão do benefício de vantagens ou auxílios públicos;

b) Interdição temporária ou permanente de exercer actividade comercial;

c) Colocação sob vigilância judicial;

d) Dissolução por via judicial.

2. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do n.º 2 do artigo 8.º seja passível de sanções ou medidas efectivas, proporcionadas e dissuasivas.

Artigo 10.º

Competência

1. Cada Estado-Membro deve definir a sua competência relativamente às infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º, sempre que a infracção tiver sido praticada:

a) Total ou parcialmente no seu território; ou

b) Por um nacional seu; ou

c) Em benefício de uma pessoa colectiva com sede no seu território.

2. Ao definir a sua competência em conformidade com a alínea a) do n.º 1, cada Estado-Membro deve assegurar que sejam incluídos os casos em que:

a) O autor praticou a infracção 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. Qualquer Estado-Membro que, nos termos do seu direito, ainda não extradite ou entregue os seus nacionais, deve tomar as medidas necessárias para definir a sua competência e, eventualmente, para instaurar procedimento penal relativamente às infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º, quando praticadas por um dos seus nacionais fora do seu território.

4. Sempre que uma infracção seja da competência de mais do que um Estado-Membro e qualquer um deles possa validamente instaurar procedimento penal com base nos mesmos factos, os Estados-Membros em causa devem cooperar para decidir qual deles moverá o procedimento contra os autores da infracção, tendo em vista centralizá-lo, se possível, num único Estado-Membro. Para o efeito, os Estados-Membros podem recorrer a qualquer órgão ou mecanismo instituído no seio da União Europeia para facilitar a cooperação entre as suas autoridades judiciais e a coordenação das respectivas acções. Serão tidos em conta, sucessivamente, os seguintes elementos:

— o Estado-Membro ser aquele em cujo território foram praticadas as infracções, nos termos da alínea a) do n.º 1 e do n.º 2,

— o Estado-Membro ser o da nacionalidade do autor,

— o Estado-Membro ser aquele em cujo território o autor foi encontrado.

5. Qualquer Estado-Membro pode decidir que não aplicará ou que só aplicará em casos ou condições específicos, as regras de competência estabelecidas nas alíneas b) e c) do n.º 1.

6. Sempre que decidirem aplicar o n.º 5, os Estados-Membros devem informar desse facto o Secretariado-Geral do Conselho e a Comissão, indicando, se necessário, os casos ou condições especiais em que a decisão se aplica.

Artigo 11.º

Intercâmbio de informações

1. Para efeitos da troca de informações relativa às infracções referidas nos artigos 2.º, 3.º, 4.º. e 5.º e de acordo com as normas em matéria de protecção de dados, os Estados-Membros devem recorrer à rede existente de pontos de contacto operacionais, disponíveis 24 horas por dia e sete dias por semana.

2. Cada Estado-Membro deve notificar ao Secretariado-Geral do Conselho e à Comissão o ponto de contacto designado para efeitos de troca de informações sobre infracções relacionadas com ataques contra sistemas de informação. O Secretariado-Geral transmite essa informação aos restantes Estados-Membros.

Artigo 12.º

Transposição

1. Os Estados-Membros devem tomar as medidas necessárias para dar cumprimento às disposições da presente decisão-quadro até 16 de Março de 2007.

2. Os Estados-Membros devem transmitir ao Secretariado-Geral do Conselho e à Comissão, até 16 de Março de 2007, o texto das disposições que transpõem para o respectivo direito nacional as obrigações resultantes da presente decisão-quadro. Até 16 de Setembro de 2007, com base num relatório elaborado a partir daquelas informações e num relatório escrito apresentado pela Comissão, o Conselho verifica em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à presente decisão-quadro.

Artigo 13.º

Entrada em vigor

A presente decisão-quadro entra em vigor na data da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 24 de Fevereiro de 2005.

Pelo Conselho

O Presidente

N. SCHMIT