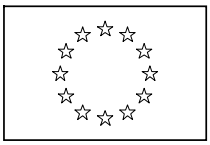

COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 19.04.2002
COM(2002)173 final

2002/0086 (CNS)

Proposta de

DECISÃO-QUADRO DO CONSELHO

relativa a ataques contra os sistemas de informação

(apresentada pela Comissão)

EXPOSIÇÃO DE MOTIVOS

1. INTRODUÇÃO

As redes de comunicações electrónicas e os sistemas de informação fazem actualmente parte integrante da vida quotidiana dos cidadãos da União Europeia e desempenham um papel fundamental no sucesso da economia europeia. As redes e os sistemas de informação convergem e estão cada vez mais interligados. Esta evolução implica vantagens numerosas e evidentes, mas é igualmente acompanhada da ameaça inquietante de ataques intencionais contra os sistemas de informação. Estes ataques podem assumir formas muito diferentes que incluem o acesso ilegal, a propagação de códigos malévolos e ataques de negação de serviço. É possível lançar estes ataques a partir de e em direcção a qualquer local do mundo e a qualquer momento. Novas formas de ataques inesperados poderão ocorrer no futuro.

Os ataques contra os sistemas informação constituem uma ameaça contra a criação de uma sociedade da informação mais segura e de um espaço de liberdade, de segurança e de justiça, sendo conveniente, portanto, dar-lhe uma resposta a nível da União Europeia. A presente proposta da decisão-quadro, relativa à aproximação do direito penal em matéria de ataques contra os sistemas de informação, increve-se no quadro do contributo da Comissão para essa resposta.

1.1. Tipos de ataques contra os sistemas de informação

A expressão “sistema de informação” é deliberadamente utilizada no presente

contexto na sua acepção mais ampla, tendo em conta a convergência entre as redes de comunicações electrónicas e os diferentes sistemas que aquelas interligam. Para efeitos da presente proposta, os sistemas de informação incluem, portanto, os computadores pessoais autónomos, as agendas digitais pessoais, os telemóveis, as intranets, as extranets e, obviamente, as redes, os servidores e outras infra-estruturas da Internet.

A Comissão, na sua Comunicação intitulada "Segurança das redes e da informação: Proposta de abordagem de uma política europeia"[1], apresentou a seguinte descrição de ameaças contra os sistemas informáticos:

(a) **Acesso não autorizado aos sistemas de informação**. Este tipo de ataque inclui a noção de “**hacking**” (pirataria informática). Esta prática consiste em aceder, sem para tal estar autorizado, a um computador ou a uma rede de computadores. Pode assumir diferentes formas, desde a mera exploração de informações internas até aos ataques brutais e à intercepção de senhas (passwords). Existe geralmente – mas nem sempre - a intenção dolosa de copiar, alterar ou destruir dados. A corrupção intencional de *sites* Internet ou o acesso sem pagamento a serviços protegidos por acesso condicional pode ser uma das finalidades da prática referida.

(b) **Perturbação dos sistemas de informação.** Existem várias formas de perturbar o funcionamento dos sistemas de informação através de ataques malévolos. Uma das formas mais conhecidas de bloquear ou degradar os serviços oferecidos pela Internet

---

[1] 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”, de 6.6.2001. COM (2001) 298 final.

consiste na "**negação de serviço**" (DoS). Este ataque é, de certa forma, análogo ao facto de inundar as telecopiadoras com numerosas mensagens longas e repetidas. Os ataques de negação de serviço visam sobrecarregar os servidores ou os fornecedores de serviços Internet (ISP) com mensagens geradas automaticamente. Outros tipos de ataques podem consistir na perturbação dos servidores que fazem funcionar o sistema de nome de domínio (DNS) ou visar os "*routers*" (encaminhadores). Os ataques destinados a perturbar os sistemas foram prejudiciais a certos *sites* respeitados da Internet como é o caso dos portais. Segundo alguns estudos, um ataque recente causou prejuízos calculados em várias centenas de milhões de euros, sem contar o prejuízo não quantificável em termos de reputação. As empresas contam cada vez mais com a disponibilidade do seu *site* Internet para os seus negócios e as que dependem desses *sites* para os fornecimentos "just in time", são particularmente vulneráveis.

(c) **Execução de *software* malévolo que altera ou destrói dados**. O tipo mais conhecido de *software* malévolo é o vírus. Os vírus "I Love You", "Melissa" e "Kournikova" constituem exemplos devastadores. Cerca de 11 % dos utilizadores europeus foi atacado por um vírus no seu computador pessoal (PC). Existem outros tipos de software malévolo. Alguns causam danos apenas ao próprio computador, enquanto que outros utilizam o PC para atacar outros elementos da rede. Alguns programas (designados 'logic bombs') podem manter-se inactivos até serem activados por um evento como uma data específica e causam graves prejuízos alterando ou destruindo dados. Outros programas têm uma aparência normal, mas quando são lançados, desencadeiam um ataque malévolo (conhecidos como 'cavalos de Tróia'). Outros programas (denominados "vermes") não infectam os restantes programas como os vírus, mas criam réplicas de si próprios que, por sua vez, continuam a reproduzir-se até afogar eventualmente o sistema.

(d) **Intercepção das comunicações**. A intercepção malévola de comunicações compromete as exigências de confidencialidade e de integridade dos utilizadores. É frequentemente denominada por "sniffing".

(e) **Identidade falsa**. Os sistemas de informação proporcionam novas oportunidades de identidades falsas e de fraude. Adoptar a identidade de outra pessoa na Internet e de a utilizar com objectivos malévolos é normalmente denominado por "spoofing".

1.2. A natureza da ameaça

É imperioso coligir informações fiáveis sobre a extensão e a natureza dos ataques contra os sistemas de informação.

Os ataques mais graves contra os sistemas de informação visam os operadores de redes de comunicações electrónicas e os fornecedores de serviços ou as empresas de comércio electrónico. Domínios mais tradicionais podem também ser gravemente afectados devido a uma cada vez maior interconexão das comunicações modernas: as indústrias transformadoras, os serviços, os hospitais, outros organismos do sector público e os próprios governos. Todavia, as vítimas dos ataques não são apenas as empresas; os ataques podem igualmente causar danos directos, graves e prejudiciais aos particulares. O ónus económico imposto por alguns destes ataques relativamente a organismos públicos, a empresas e a particulares é também significativo, arriscando-se a tornar os sistemas de informação mais onerosos e menos acessíveis aos utilizadores.

Os tipos de ataques acima descritos são frequentemente praticados por indivíduos que actuam por sua própria conta, por vezes menores que não podem avaliar plenamente a gravidade dos seus actos. Todavia, os níveis de sofisticação e de ambição dos ataques poderão aumentar. Existe o receio crescente e preocupante de que grupos criminosos organizados utilizem as redes de comunicações para lançar ataques contra os sistemas de informação em seu próprio benefício. Os grupos organizados de "hacking", especializados na pirataria informática e na degradação dos *sites* Internet, são cada vez mais activos a nível mundial. Trata-se, por exemplo, do caso dos "Brazilian Silver Lords" e dos "Pakistan Gforce", que tentam extorquir dinheiro às suas vítimas, propondo-lhes uma assistência especializada após o "hacking" dos seus sistemas de informação. A prisão de importantes grupos de "hackers" sugere que esta prática poderá, cada vez mais, constituir um fenómeno de criminalidade organizada. Recentemente, verificaram-se ataques sofisticados e organizados contra direitos de propriedade intelectual e tentativas de desviar montantes consideráveis a instituições bancárias[2].

As violações da segurança das bases de dados de *sites* de comércio electrónico que dão acesso a informações sobre clientes, incluindo números de cartões de crédito, são igualmente preocupantes. Estes ataques aumentam as possibilidades de fraude em matéria de pagamentos e obrigam inevitavelmente os bancos a anular e a voltar a emitir milhares de cartões. Têm igualmente por consequência causar um prejuízo não quantificável à reputação do *site* e à confiança dos consumidores no comércio electrónico. Medidas de prevenção, designadamente condições mínimas de segurança impostas às empresas em linha que aceitam os pagamentos através de cartões bancários, estão a ser examinadas no quadro do plano de acção de combate à fraude e à falsificação dos meios de pagamento que não em numerário[3] .

A presente proposta constitui igualmente parte do contributo da Comissão para a resposta à ameaça de um ataque terrorista contra sistemas de informação vitais na União Europeia. Completa as propostas da Comissão visando substituir, na União Europeia, o procedimento de extradição por um mandado de captura europeu[4] e aproximar as legislações em matéria de terrorismo[5] que foram objecto de um acordo político no Conselho Europeu de Laeken, de 14 e 15 de Dezembro de 2001. Considerados conjuntamente, estes instrumentos garantirão que os Estados-Membros da União Europeia disponham de um direito penal eficaz para lutar contra o ciberterrorismo e reforçarão a cooperação internacional contra o terrorismo.

A presente proposta não abrange apenas os actos dirigidos contra os Estados-Membros. É igualmente aplicável a actos perpetrados no território da União Europeia visando sistemas de informação situados no território de países terceiros. Esta medida reflecte o compromisso assumido pela Comissão de combater os ataques contra sistemas de informação tanto a nível mundial como a nível da União Europeia.

---

2 Segundo um inquérito publicado pela "Communications Management Association (CMA)", já foram praticados ataques sob a forma de "hacking" contra um terço das grandes empresas e organismos do sector público do Reino Unido, incluindo os serviços governamentais, causando danos como a infiltração de contas bancárias de empresas ou roubo de informação. Ver o inquérito sobre o *site* seguinte: http:/www.cma.org.

3 Comunicação da Comissão "Combate à fraude e à falsificação dos meios de pagamento que não em numerário", COM (2001) 11 final. Adoptada pela Comissão em 9.2.2001.

4 Proposta de decisão-quadro do Conselho relativa ao mandado de captura europeu. COM(2001) 522 final. Adoptada pela Comissão em 19.9.2001.

5 Proposta de decisão-quadro do Conselho relativa à luta contra o terrorismo. COM(2001) 521 final. Adoptada pela Comissão em 19.9.2001.

De facto, em várias ocasiões recentes, as tensões nas relações internacionais implicaram um recrudescimento dos ataques contra os sistemas de informação, envolvendo frequentemente ataques contra *sites* Internet. Ataques mais graves poderiam não só ter importantes consequências financeiras mas, em alguns casos, implicar igualmente a perda de vidas humanas caso visem, por exemplo, sistemas hospitalares ou sistemas de controlo do tráfico aéreo. A importância que os Estados-Membros atribuem a esta problemática resulta da prioridade concedida a várias iniciativas de protecção das infra-estruturas vitais. Por exemplo, o programa comunitário relativo às tecnologias da sociedade de informação (SIT)[6] criou, em ligação com o Departamento de Estado dos Estados Unidos, uma Task Force conjunta UE/Estados Unidos relativa à protecção das infra-estruturas vitais[7].

1.3. Necessidade de informações e estatísticas rigorosas

Existem poucas estatísticas fiáveis sobre a verdadeira grandeza do fenómeno da criminalidade informática. O número de intrusões detectadas e assinaladas até hoje não dá provavelmente uma ideia exacta da amplitude do problema. Segundo um inquérito americano[8], em 1999 só 32% das empresas que respondeu terem sido vítimas de uma intrusão informática no ano anterior assinalou o facto às autoridades. Tratou-se, no entanto, de um progresso relativamente aos anos anteriores, durante os quais apenas 17% das empresas em causa denunciou tal facto às autoridades. Há várias razões que justificam este silêncio. Muitas intrusões não são detectadas devido à falta de sensibilização e de experiência dos administradores de sistemas e dos utilizadores. Além disso, muitas empresas não estão dispostas a assinalar os casos de abusos informáticos, a fim de evitar qualquer publicidade desfavorável e a exposição ao risco de novos ataques. Os serviços policiais, na sua maioria, ainda não dispõem de estatísticas sobre a utilização de computadores e de sistemas de comunicação envolvidos neste tipo de delinquência e noutras formas de criminalidade[9]. As autoridades repressivas não têm a formação adequada para detectar e identificar as infracções informáticas e investigar este tipo de crimes. Todavia, a União Europeia iniciou a análise desta questão, coligindo dados quantificados relativos aos ataques contra os sistemas de informação. Um Estado-Membro considera que, em 1999, foram praticados entre 30 000 e 40 000 ataques contra os sistemas de informação, enquanto que apenas 105 queixas oficiais foram registadas neste domínio. Em 1999, sete Estados-Membros registaram um total de apenas 1844 denúncias oficiais de infracções praticadas contra sistemas de informação e dados informáticos. Tal corresponde, contudo, a uma duplicação do número de infracções assinaladas em 1998, ano em que apenas 972 casos foram registados oficialmente nestes sete Estados-Membros[10].

---

6 O programa TSI é gerido pela Comissão Europeia. Faz parte do quinto programa-quadro, que cobre o período de 1998 a 2002. Para mais informações, consultar o *site* t http://www.cordis.lu/ist.

7 Sob a égide do grupo consultivo conjunto criado por força do acordo de cooperação científica e tecnológica entre a Comunidade Europeia e o Governo dos Estados Unidos da América.

8 O "Computer Security Institute (CSI)" e o "Federal Bureau of Investigation (FBI)" publicam no início de cada ano o "Computer Crime and Security Survey". Ver o *site* do CSI e outras informações sobre o inquérito em **www. gocsi.com**

9 O Ministério do Interior italiano publicou recentemente estatísticas sobre as suas actividades operacionais contra a criminalidade informática em 1999 e 2000 (ver http://www.mininterno.it/dip_ps/dcpsffp/index.htm). Os registos oficiais de casos de pirataria informática foram em 2000 de 98, ou seja, quatro vezes mais do que em 1999, ano em que apenas foram oficialmente registados 21 casos.

10 Documento do Conselho 8123/01 ENFOPOL 38. Disponível no *site* Internet do Conselho http://db.consilium.eu.int/jai

Além disso, um inquérito recente[11] revelou que 13% por cento das empresas vítimas da criminalidade económica indicou que uma das infracções correspondia à figura da criminalidade informática. Este inquérito revela igualmente uma inquietação crescente associada à criminalidade informática, pois 43% das respostas menciona a cibercriminalidade como um risco futuro. Outro estudo concluiu que os "hackers" e os vírus constituem a maior ameaça de cibercriminalidade para as empresas, sendo os principais autores de infracções os "hackers" (45%), os antigos empregados (13%), os grupos de criminalidade organizada (13%) e os actuais empregados (11%)[12]. Estes valores deverão continuar a aumentar devido à utilização acrescida de sistemas de informação, à interligação crescente, acompanhadas da maior vontade de assinalar os ataques. Todavia, é evidente que devem ser tomadas medidas urgentes tendo em vista elaborar um instrumento estatístico que possa ser utilizado em todos os Estados-Membros, a fim de que a criminalidade informática na União Europeia possa ser avaliada em termos quantitativos e qualitativos. O ponto de partida para esse tipo de análise consiste numa definição comum, a nível da União Europeia, das infracções que envolvem ataques contra os sistemas de informação.

1.4. Contexto político na União Europeia

Neste contexto, no Conselho Europeu de Lisboa de Março de 2000, o Conselho Europeu sublinhou a importância que reveste a transição para uma economia competitiva, dinâmica e baseada no conhecimento, tendo convidado o Conselho e a Comissão a elaborar um plano global de acção *e*Europe para daí retirar o máximo de benefícios[13]. Este plano de acção, preparado pela Comissão e pelo Conselho e aprovado pelo Conselho Europeu da Feira, em Junho de 2000, compreende acções destinadas a reforçar a segurança das redes e prevê a elaboração de uma abordagem coordenada e coerente da criminalidade informática até final de 2002.

No quadro do seu contributo para este mandato relativo à cibercriminalidade, a Comissão publicou a Comunicação intitulada "Criar uma sociedade da informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade"[14]. É proposta uma abordagem equilibrada de análise dos problemas da cibercriminalidade que toma plenamente em conta os pareceres de todas as partes interessadas, incluindo as entidades encarregues da aplicação da lei, os fornecedores de acesso, os operadores de redes, outros grupos industriais, as associações de consumidores, as autoridades responsáveis pela protecção de dados e as associações de protecção da vida privada. A comunicação propõe um determinado número de iniciativas legislativas e não-legislativas.

O programa IDA, no âmbito do qual os Estados-Membros e a Comissão já estão trabalhar a nível de uma política de segurança comum e da criação de uma rede de intercâmbio de informações administrativas segura, constitui um importante exemplo da acção actualmente em curso.

Uma das principais questões abordadas na referida comunicação dizia respeito à necessidade de uma acção eficaz para responder às ameaças contra a autenticidade, a integridade, a

---

11 European Economic Crime Survey 2001, PricewaterhouseCoopers 2001 (http://www.pwcglobal.com)

12 "The Cybercrime Survey 2001, Confederation of British Industry" (ver http://www.cbi.org.uk)

13 Conclusões da Presidência, Conselho Europeu de Lisboa, de 23 e 24 de Março de 2000, disponível no *site:* http://ue.eu.int/en/Info/eurocouncil/index.htm.

14 COM (2000) 890 final.

confidencialidade e a disponibilidade dos sistemas de informação e das redes. Foram alcançados grandes progressos em direito comunitário. A nível comunitário, já estão em vigor várias medidas jurídicas com implicações específicas para a segurança das redes e da informação.

A presente decisão-quadro completa os progressos já realizados no domínio da legislação comunitária de protecção dos sistemas de informação, nomeadamente, a Directiva 95/46/CE, a Directiva 97/66/CE e a Directiva 98/84/CE relativa à protecção jurídica dos serviços que se baseiem ou consistam num acesso condicional. Em especial, o quadro europeu relativo às telecomunicações e à protecção de dados (Directivas 95/46/CE e 97/66/CE[15]) prevê disposições visando garantir que os fornecedores de serviços de telecomunicações acessíveis ao público sejam obrigados a adoptar medidas técnicas e de organização adequadas para assegurar a protecção, a segurança e a confidencialidade dos seus serviços e um nível de segurança correspondente ao eventual risco.

A prevenção e a educação constituem as formas mais importantes e eficazes de abordar estes problemas. A citada comunicação sublinha a relevância da disponibilidade, da criação, do funcionamento e da utilização eficaz de tecnologias de prevenção. A comunicação realça que é necessário sensibilizar o público para os riscos associados à criminalidade informática, promover as melhores práticas em matéria de segurança das tecnologias da informação, definir instrumentos e procedimentos eficazes, a fim de lutar contra a criminalidade informática, bem como encorajar os desenvolvimentos em matéria de mecanismos de alerta rápido e de gestão de crises. O programa comunitário relativo às tecnologias da sociedade de informação (TSI)[16], fornece um quadro para o desenvolvimento das capacidades e das técnicas necessárias para compreender e dar resposta aos desafios que a criminalidade informática começa a colocar.

Mais recentemente, o Conselho Europeu de Estocolmo, de 23 e 24 de Março, reconheceu a necessidade de acções complementares no domínio da segurança das redes e das informações, concluindo que, *"o Conselho, em conjunto com a Comissão, desenvolverá uma estratégia global sobre a segurança das redes electrónicas, incluindo medidas práticas de execução a apresentar ao Conselho Europeu de Gotemburgo"*. A Comissão respondeu a este pedido com a Comunicação intitulada "Segurança das redes e da informação: Proposta de abordagem de uma política europeia"[17]. Esta comunicação analisa os problemas actuais em matéria de segurança das redes e define um quadro estratégico de acção neste domínio. Em seguida, o Conselho adoptou uma resolução em 6 de Dezembro de 2001 sobre uma abordagem comum e acções específicas no domínio da segurança das redes e da informação.

Estas iniciativas não são suficientes para, por si só, fornecerem todas as respostas necessárias aos ataques graves contra os sistemas de informação. Ambas as comunicações da Comissão reconheceram igualmente que seria urgente aproximar o direito penal material dos Estados-Membros da União Europeia em matéria de ataques contra os sistemas de informação. Foram assim tidas em conta as conclusões do Conselho Europeu de Tampere de Outubro de 1999[18], que incluiu a criminalidade que recorre a tecnologias avançadas numa lista limitada de sectores relativamente aos quais devem ser desenvolvidos esforços para alcançar um acordo sobre definições, incriminações e sanções comuns, bem como a

---

15 JO L 281 de 23.11.1995, pp. 31-50, JO L 24 de 30.01.1998, pp. 1 a 8.

16 O programa TSI é gerido pela Comissão Europeia. Faz parte do quinto programa-quadro, que cobre o período de 1998 a 2002. Para mais informações, consultar o *site* http://www.cordis.lu/ist.

17 COM (2001) 298 final, de 6 de Junho de 2001.

18 http://db.consilium.eu.int/en/Info/eurocouncil/index.htm.

recomendação nº 7 da estratégia da União Europeia relativa à prevenção e controlo da criminalidade organizada para o novo milénio, que foi adoptada pelo Conselho JAI em Março de 2000[19]. A presente proposta de decisão-quadro faz igualmente parte do programa de trabalho da Comissão para 2001[20] e do painel de avaliação dos progressos realizados na criação de uma espaço de liberdade, segurança e justiça na União Europeia, apresentado pela Comissão em 30 de Outubro de 2001[21].

1.5. Necessidade de aproximação do direito penal dos Estados-Membros

Neste domínio, os direitos penais dos Estados-Membros apresentam lacunas jurídicas e diferenças importantes susceptíveis de impedir a luta contra a criminalidade organizada e o terrorismo, bem como ataques graves contra os sistemas de informação praticados por particulares. A aproximação dos direitos materiais em matéria de criminalidade que utiliza as tecnologias avançadas, garantirá que as legislações nacionais sejam suficientemente completas para que todas as formas de ataques graves contra os sistemas de informação possam ser objecto de inquéritos recorrendo a técnicas e métodos disponíveis em direito penal. Os autores destas infracções devem ser identificados e processados, devendo os tribunais dispor de sanções adequadas e proporcionadas. Este tipo de medidas permitirá enviar uma forte mensagem dissuasiva aos potenciais autores de ataques contra os sistemas de informação.

Além disso, as lacunas jurídicas e as diferenças entre os vários regimes podem impedir uma cooperação policial e judiciária eficaz no caso de ataques contra os sistemas de informação. Estes são frequentemente transnacionais por natureza, necessitando de uma cooperação policial e judiciária internacional. A aproximação das legislações melhorará, assim, essa cooperação, garantindo que a exigência de dupla incriminação fique preenchida (nos termos da qual determinado comportamento deve constituir uma infracção nos dois países considerados para que estes últimos possam ajudar-se mutuamente a nível judiciário no quadro de um inquérito penal). Esta iniciativa permitirá aos Estados-Membros da UE reforçar a sua cooperação recíproca e reforçar a cooperação com os países terceiros (caso tenha sido celebrado um acordo mútuo de assistência judiciária).

É igualmente necessário completar os instrumentos existentes a nível da União Europeia. A Decisão-quadro do Conselho relativa ao mandado de captura europeu[22], o Anexo à Convenção Europol[23] e a Decisão do Conselho que cria a Eurojust[24], compreendem referências à criminalidade informática que convém definir de forma mais rigorosa. Para efeitos destes 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[25] que abrange as infracções terroristas causadoras de danos graves a

---

19 "Prevenção e controlo da criminalidade organizada: Estratégia da União Europeia para o início do novo milénio (JO C 124 de 3.5.2000).

20 http://europa.eu.int/comm/off/work_programme/index_en.htm

21 http://europa.eu.int/comm/dgs/justice_home [COM (2001) 628 final, de 30.10.2001].

22 JO C , p. .

23 Acto do Conselho, de 26 de Julho de 1995, que estatui a Convenção elaborada com base no artigo K.3 do Tratado da União que cria um Serviço Europeu de Polícia (Convenção Europol) - JO C 316, de 27.11.1995, p. 1.

24 JO C , p. .

25 JO C , p. .

uma infra-estrutura, incluindo um sistema de informação, e susceptíveis de colocar em risco a vida de pessoas ou causar importantes prejuízos económicos.

1.6. Âmbito de aplicação e objecto da decisão-quadro

Os objectivos da presente decisão-quadro do Conselho consistem, portanto, em aproximar o direito penal dos Estados-Membros em matéria de ataques contra os sistemas de informação e assegurar a melhor cooperação policial e judiciária possível no que diz respeito às infracções penais que consistem em ataques contra os sistemas de informação. Além disso, a presente proposta é um contributo para os esforços da União Europeia de combate contra a criminalidade organizada e o terrorismo. Não se pretende exigir que os Estados-Membros criminalizem comportamentos pouco graves ou insignificantes.

Resulta claramente do artigo 47º do Tratado da União Europeia que a presente decisão-quadro não contraria o disposto no direito comunitário. Em especial, não afecta os direitos à vida privada ou à protecção de dados e as obrigações previstas pelo direito comunitário (por exemplo, directivas 95/46 e 97/66). Não se pretende que os Estados-Membros criminalizem as infracções que têm por objecto o acesso ou a divulgação de dados com carácter pessoal, a confidencialidade das comunicações, a segurança do tratamento de dados com carácter pessoal, as assinaturas electrónicas[26] ou as violações de direitos de propriedade intelectual, não afectando o disposto na Directiva 98/84/CE relativa à protecção jurídica dos serviços que se baseiem ou consistam num acesso condicional[27]. Trata-se de questões importantes, mas que já são abrangidas pelo direito comunitário em vigor. Qualquer aproximação do direito penal nestes domínios tendo em vista objectivos legislativos comunitários, nomeadamente a protecção de dados com carácter pessoal, a remuneração do fornecimento de serviços ou a propriedade intelectual deve, por conseguinte, ser prevista no quadro do direito comunitário e não no quadro do Título VI do Tratado da UE. Por conseguinte, a presente decisão-quadro abrange apenas os comportamentos descritos nos pontos a) a c) da secção 1.1.

A acção legislativa a nível da União Europeia deve ter igualmente em conta a situação noutras instâncias internacionais. No contexto da aproximação do direito penal material relativo aos ataques contra sistemas de informação, é actualmente o Conselho da Europa que se encontra mais avançado. Desde Fevereiro de 1997 que se iniciou a elaboração de uma convenção internacional sobre a cibercriminalidade, a qual foi formalmente adoptada e aberta para assinatura em Novembro de 2001[28]. A convenção visa aproximar uma série de infracções penais, designadamente infracções contra a confidencialidade, a integridade e a disponibilidade de sistemas e de dados informáticos. A presente decisão-quadro pretende ser coerente com a abordagem adoptada na convenção do Conselho Europa em relação a estas infracções.

Aquando dos debates do G8 sobre a criminalidade que utiliza as tecnologias avançadas, foram identificadas duas categorias principais de ameaças. Trata-se, em primeiro lugar, das ameaças com que se confrontam as infra-estruturas informáticas, consistindo em operações destinadas a interromper, negar, corromper ou destruir informações existentes em computadores e redes de computadores ou destinados a afectar os próprios computadores e redes. Em segundo

---

[26] Directiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinatura electrónicas, JO L 13 de 19.01.2000.

[27] JO L 320 de 28.11.1998, pp. 54 a 57.

[28] O texto está disponível na Internet, em duas línguas, respectivamente francês e inglês: http://conventions.coe.int/treaty/fr/projets/cybercrime.htm.
http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

lugar, as ameaças assistidas por computador, ou seja, actividades dolosas, designadamente as fraudes, o branqueamento de capitais, a pornografia infantil, a violação dos direitos de propriedade intelectual e o tráfico de droga, facilitadas graças à utilização de um computador. A presente proposta abarca a primeira categoria de ameaças.

A aproximação a nível da UE deverá ter em conta a evolução da problemática nas instâncias internacionais e deverá ser conforme com as actuais políticas comunitárias. A presente proposta tem igualmente por objectivo alcançar uma maior aproximação das legislações na UE do que foi possível obter a nível de outras instâncias internacionais.

2. BASE JURÍDICA

O objectivo que consiste em criar um espaço de liberdade, de segurança e de justiça deve ser realizado através da prevenção e da luta contra a criminalidade, organizada ou não, incluindo o terrorismo, graças a uma cooperação mais estreita entre os serviços repressivos e as autoridades judiciárias dos Estados-Membros e a uma aproximação das disposições penais dos Estados-Membros. A presente proposta de decisão-quadro visa, portanto, a aproximação das disposições legislativas e regulamentares dos Estados-Membros em matéria de cooperação policial e judiciária penal. Prevê "normas mínimas respeitantes aos elementos constitutivos das infracções penais", em larga medida em matéria de criminalidade organizada e de terrorismo. Visa igualmente "garantir a compatibilidade das normas aplicáveis nos Estados-Membros" tendo em vista facilitar e acelerar a cooperação entre as autoridades judiciárias. A base jurídica indicada no preâmbulo da proposta compreende, assim, o artigo 29º, a alínea a) do artigo 30º, o artigo 31º e o nº 2, alínea b), do artigo 34º do Tratado da União Europeia. A presente proposta não terá incidências financeiras sobre o orçamento das Comunidades Europeias.

3. A DECISÃO-QUADRO: ARTIGOS

Artigo 1º - Âmbito de aplicação e objectivo da decisão-quadro

Este artigo indica expressamente que a decisão-quadro tem por objectivos aproximar o direito penal dos Estados-Membros em matéria de ataques graves contra os sistemas de informação, em especial contribuir para a luta contra a criminalidade organizada e o terrorismo e, com esta medida, assegurar que a cooperação judiciária seja a mais estreita possível no que diz respeito às infracções penais em matéria de ataques contra os sistemas de informação. Em conformidade com o artigo 47º do Tratado da União Europeia, a presente decisão-quadro também não afecta o direito comunitário. Tal inclui, designadamente, o direito à vida privada e à protecção de dados, bem como as obrigações previstas pelas directivas 95/46 e 97/66. A decisão-quadro não visa exigir dos Estados-Membros que criminalizem as infracções em matéria de acesso/divulgação de dados com carácter pessoal, de confidencialidade das comunicações, de segurança do tratamento de dados com carácter pessoal, de assinaturas electrónicas[29] ou de violações dos direitos de propriedade intelectual, não afectando o disposto na Directiva 98/48/CE relativa à protecção jurídica dos serviços que se baseiem ou consistam num acesso condicional[30].

---

[29] Directiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinatura electrónicas, JO L 13 de 19.01.2000.

[30] JO L 320 de 28.11.1998, pp. 54 a 57.

A presente decisão-quadro não impõe aos Estados-Membros que criminalizem comportamentos sem gravidade ou insignificantes. Os seus artigos 3º e 4º definem os critérios que devem estar preenchidos para que determinado comportamento seja criminalizado. Estes critérios respeitam as possibilidades de derrogação e de reserva previstas no projecto de convenção do Conselho da Europa relativa à cibercriminalidade

Todas infracções penais abrangidas pela decisão-quadro devem ter sido praticadas de forma intencional. O termo "intencional" é utilizado expressamente nos artigos 3º, 4º e 5º. Convém interpretá-lo em conformidade com os princípios normais de direito penal dos Estados-Membros que regulam a figura do dolo. Assim, a presente decisão-quadro não exige a criminalização de acções no caso de negligência grave ou outra incúria, mas sem carácter intencional. A intenção de aceder a sistemas de informação ou de os perturbar de forma ilícita deverá ser em geral suficiente, não sendo necessário provar que o acto intencional visava um sistema de informação específico.

Artigo 2º - Definições

A proposta de decisão-quadro do Conselho compreende as seguintes definições:

a) "*Rede de comunicações electrónicas*". É utilizada a mesma definição adoptada na Directiva do Conselho e do Parlamento Europeu, de 14 de Fevereiro de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas[31].

b) *"Computador"*. Esta definição tem por base o artigo 1º do projecto de convenção do Conselho da Europa relativa à cibercriminalidade. A definição abrange também, por exemplo, os computadores pessoais autónomos, as agendas digitais e pessoais, descodificadores digitais, vídeo-gravadores pessoais e os telemóveis (caso tenham funções de tratamento de dados, WAP e de terceira geração), que não estejam inteiramente cobertos pela definição de redes de comunicações electrónicas.

c) *"Dados informáticos"*. Esta definição tem por base a definição dos dados da ISO[32]. Não se pretende abranger com esta definição dados físicos como, por exemplo, livros. Contudo, inclui livros armazenados sob a forma de dados informáticos (ou seja, salvaguardados num formato electrónico como um ficheiro de tratamento de texto) ou convertidos em dados informáticos através de leitura óptica (scanning). Por esta razão, a definição especifica que os dados informáticos devem ter sido "criados ou inseridos sob uma forma" susceptível de ser tratada por um sistema de informação ou permitir a um sistema de informação executar uma função.

d) *"Sistema de informação"*. A definição de sistema de informação é originariamente inspirada na definição adoptada pela OCDE em 1992 nas suas orientações relativas à segurança dos sistemas de informação ("Guidelines for the Security of Information Systems") e em definições anteriores que fazem referência às redes de comunicações electrónicas, aos computadores e aos dados informáticos. Esta expressão tinha sido igualmente utilizada em instrumentos de direito comunitário anteriores, nomeadamente a Decisão do Conselho, de 31 de Março de 1992, "em matéria de

---

31 Ver o texto final em http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg

32 A Organização Internacional de Normalização (ISO) é uma federação mundial de organismo nacionais de normalização a que pertencem cerca de cem países.

segurança dos sistemas de informação" e a recomendação do Conselho, de 7 de Abril de 1995, "relativa aos critérios comuns destinados a avaliar o grau de confiança dos sistemas de informação". Pretende-se que a referida expressão seja tecnologicamente neutra e que traduza com rigor o conceito de redes e de sistemas interligados contendo dados. É abrangido tanto o *hardware* como o *software* do sistema, sem no entanto incluir o conteúdo da própria informação. Abrange igualmente os sistemas autónomos. A Comissão considera que é preferível alargar a protecção concedida pelo direito penal aos computadores autónomos, não a limitando apenas aos sistemas interligados.

e) *"Pessoa colectiva"*. Trata-se de uma definição habitual constante de decisões-quadro anteriores do Conselho.

f) "*Pessoa autorizada*". Trata-se da pessoa 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. Pode tratar-se de pessoas que actuam em conformidade com a autorização legal de outra pessoa à qual foi conferida tal autorização expressa. É especialmente importante que as seguintes categorias de pessoas e de actividades legítimas (no limite dos direitos, autorizações e responsabilidades das pessoas e em conformidade com as normas comunitárias que regulam a protecção de dados e a confidencialidade das comunicações) não sejam criminalizadas quando a presente decisão-quadro vier a ser transposta para o direito nacional:

- os actos dos utilizadores habituais, quer se trate de particulares ou de empresas, incluindo o recurso à cifragem para proteger as suas próprias comunicações e dados;
- as técnicas de retro-engenharia, nos limites previstos pela Directiva 91/250, de 14 de Maio de 1991, "relativa à protecção jurídica dos programas de computador"[33];
- os actos dos administradores, verificadores e operadores de redes e de sistemas;
- os actos de pessoas autorizadas que procedem ao teste de um sistema, no âmbito de uma empresa, ou de pessoas nomeadas externamente e autorizadas a testar a segurança de determinado sistema;
- a investigação científica legítima.

g) "*Sem ter o direito*". Trata-se de uma noção ampla e que permite uma relativa liberdade por parte dos Estados-Membros para definirem com rigor a infracção. Todavia, a fim de facilitar a transposição da decisão-quadro do Conselho para as legislações nacionais, a Comissão considera necessário indicar que determinadas actividades não deverão constituir infracções. Não é possível, e provavelmente não será desejável, estabelecer uma lista de isenções exaustiva e limitativa a nível da União Europeia. No entanto, a expressão "sem ter o direito", completa as definições anteriores de forma a excluir os actos de pessoas autorizadas. Exclui igualmente qualquer outro comportamento cujo carácter lícito é reconhecido pelo direito

---

33 JO L 122 de 17.05.1991, pp. 42 a 46.

nacional, incluindo os mecanismos de defesa jurídica e outros meios de defesa reconhecidos em direito nacional.

Artigo 3º - Ataques através de acesso ilícito aos sistemas de informação

Esta infracção abrange o acesso ilícito aos sistemas de informação e a noção de "hacking". Os Estados-Membros são livres de excluir os casos sem gravidade ou insignificantes do âmbito da infracção quando procederem à transposição da decisão-quadro para o direito nacional.

A infracção só deve ser prevista no direito nacional dos Estados-Membros se tiver sido praticada:

(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.

A Comissão não pretende de forma alguma contrariar a importância que confere à utilização de medidas técnicas eficazes para proteger os sistemas de informação. Não obstante, é lamentável que grande parte dos utilizadores se exponha a ataques por não possuir uma protecção técnica adequada (ou mesmo nenhuma protecção). Tendo em vista dissuadir os ataques contra estes utilizadores, o direito penal deve cobrir o acesso não autorizado aos seus sistemas, mesmo que estes não beneficiem de uma protecção técnica adequada. Por esta razão, e desde que exista uma intenção de causar danos ou de obter um benefício económico, não se exige que tenham sido violadas medidas de segurança para que se configure a prática da infracção.

Artigo 4º - Interferência ilícita nos sistemas de informação

Esta infracção abrange a prática intencional, sem ter o direito, de algum dos seguintes comportamentos:

a) o facto de, sem ter o direito, perturbar gravemente o funcionamento de um sistema de informação introduzindo, transmitindo, danificando, apagando, deteriorando, alterando ou suprimindo dados informáticos. A introdução ou a transmissão de dados informáticos visa especificamente o problema dos "ataques de negação de serviços", que consiste em tentar deliberadamente submergir o sistema de informação. A infracção cobre igualmente a "interrupção" do funcionamento de um sistema de informação, que se poderia deduzir da expressão "perturbar", mas que é mencionada expressamente para efeitos de clareza. Os outros elementos da infracção (danificar, apagar, deteriorar, alterar ou suprimir dados informáticos) cobrem especificamente o problema dos vírus e de outros tipos de ataques, que visam perturbar ou mesmo interromper as funções do próprio sistema de informação.

b) o facto de apagar, deteriorar, alterar, suprimir ou tornar inacessíveis dados informáticos de um sistema de informação, quando é praticado com a intenção de causar danos a uma pessoa singular ou colectiva. Esta alínea abrange os ataques através de vírus visando o conteúdo (ou dados informáticos) do sistema de informação, bem como a degradação de *sites* Internet.

A alínea a) utiliza a expressão "perturbar ou interromper gravemente" como elemento constitutivo da infracção tendo em vista descrever os efeitos desse tipo de ataque. A expressão "perturbar gravemente" não é objecto de definição, devido ao facto de poder assumir diferentes formas e o seu nível poder variar em função do tipo de ataque e das capacidades técnicas do sistema de informação atacado. Cada Estado-Membro determinará quais são os critérios que devem estar preenchidos para que um sistema de informação seja considerado "gravemente perturbado". Todavia, problemas ou perturbações menores do funcionamento dos serviços não deveriam ser considerados como preenchendo o critério de gravidade.

Tal como foi acima referido, os Estados-Membros podem excluir casos sem gravidade ou insignificantes da qualificação da infracção para efeitos da transposição da presente decisão-quadro para o direito nacional.

Artigo 5º - Instigação, ajuda, cumplicidade e tentativa

O nº 1 do artigo 5º estabelece que os Estados-Membros devem punir a instigação ou a ajuda intencional à prática das infracções contra sistemas de informação mencionadas nos artigos 3º e 4º, bem como a cumplicidade ou a tentativa de prática intencional destas infracções.

O nº 2 do artigo 5º visa especificamente a tentativa. Por força desta disposição, os Estados-Membros devem assegurar que as tentativas de prática de algumas das infracções contra os sistemas de informação mencionadas nos artigos 3º e 4º sejam puníveis.

Artigo 6º – Sanções

O nº 1 exige que os Estados-Membros tomem as medidas necessárias para que as infracções mencionadas nos artigos 3º a 5º sejam puníveis com penas efectivas, proporcionadas e dissuasivas[34].

Por força deste número, os Estados-Membros devem prever sanções proporcionadas à gravidade da infracção, compreendendo penas privativas de liberdade, cuja pena máxima não pode ser inferior a um ano nos casos graves. Deve considerar-se que estes excluem os comportamentos que não causaram quaisquer danos ou benefícios económicos.

A sanção máxima consistindo numa pena de prisão não inferior a um ano para casos graves, implica que estas infracções são abrangidas pelo âmbito de aplicação do mandado de captura europeu, bem como de outros instrumentos, designadamente a Decisão-quadro do Conselho, de 26 de Junho de 2001[35], relativa ao branqueamento de capitais, à identificação, detecção, congelamento, apreensão e perda dos instrumentos e produtos do crime.

Tendo em conta a natureza das decisões-quadro, que vinculam os Estados-Membros quanto ao resultado a alcançar, deixando-lhes a competência quanto à forma e aos meios, os Estados-Membros conservam um relativo grau de flexibilidade para adaptar a sua legislação a estas normas e para determinar o grau de severidade das sanções aplicáveis, nos limites fixados pela decisão-quadro e, nomeadamente, as circunstâncias agravantes mencionadas no artigo 7º. A Comissão sublinha que incumbe aos Estados-Membros estabelecer os critérios

---

[34] Esta frase é retirada do acórdão proferido pelo Tribunal de Justiça, em 21 de Setembro de 1989, no processo 68/88, Colectânea 1989, p. 2965.

[35] JO L 182 de 5.7.2001, p.1.

susceptíveis de determinar o grau de gravidade de uma infracção, com base nos seus sistemas jurídicos respectivos.

As sanções não devem necessariamente consistir em penas privativas de liberdade. O nº 2 prevê a possibilidade de os Estados-Membros aplicarem multas em complemento ou substituição de penas de prisão, em conformidade com as suas tradições e sistemas jurídicos respectivos.

Artigo 7º - Circunstâncias agravantes

Este artigo prevê que os Estados-Membros possam, em determinadas circunstâncias, agravar as penas estabelecidas no artigo 6º. A Comissão sublinha que a lista das circunstâncias agravantes prevista por este artigo não afecta qualquer outra circunstância considerada agravante pela legislação do Estado-Membro em causa. A lista tem em conta circunstâncias agravantes visadas pelas disposições nacionais dos Estados-Membros e previstas nas propostas de decisões-quadro anteriores da Comissão.

Se alguma das condições seguintes indicadas no nº 1 estiver preenchida, então a pena máxima de prisão não pode ser inferior a quatro anos:

a) se a infracção foi praticada no âmbito de uma organização criminosa tal como definida pela Acção Comum 98/733/JAI, independentemente da pena aí referida;

b) se a infracção causou ou teve por resultado importantes prejuízos económicos, directos ou indirectos, lesões corporais a uma pessoa singular ou danos consideráveis numa parte das infra-estruturas vitais do Estado-Membro em causa; ou

c) a infracção gerou lucros importantes.

Os Estados-Membros devem igualmente assegurar que as infracções referidas nos artigos 3°, 4° e 5° sejam puníveis com penas privativas de liberdade superiores às que estão previstas no artigo 6° quando o autor da infracção tenha sido condenado mediante sentença transitada em julgado num Estado-Membro.

Artigo 8º - Circunstâncias especiais

Este artigo prevê circunstâncias especiais, nos termos das quais um Estado-Membro pode decidir reduzir as penas referidas nos artigos 6º e 7º se as autoridades judiciárias competentes considerarem que o autor da infracção apenas causou um dano pouco significativo.

Artigo 9º - Responsabilidade das pessoas colectivas

Em conformidade com a abordagem de alguns instrumentos jurídicos adoptados a nível da UE para lutar contra diferentes tipos de criminalidade, convém igualmente abranger a situação em que pessoas colectivas estão implicadas em ataques contra sistemas de informação. Assim, o artigo 9º contém disposições que permitem responsabilizar uma pessoa colectiva pelas infracções mencionadas nos artigos 3º, 4º e 5º, se forem praticadas em seu benefício por uma pessoa actuando em nome individual ou enquanto membro de um órgão da pessoa colectiva em causa, que ocupa uma função dirigente. Por "responsabilidade", entende-se quer a responsabilidade penal, quer a responsabilidade civil.

Além disso, segundo uma prática habitual, o nº 2 prevê que uma pessoa colectiva possa ser igualmente considerada responsável sempre que a falta de vigilância ou de controlo, por parte da pessoa em condições de o exercer, tenha tornado possível a prática das infracções em seu benefício. O nº 3 indica que uma acção judicial contra a pessoa colectiva não exclui a possibilidade de procedimento paralelo contra uma pessoa singular.

Artigo 10º - Sanções aplicáveis às pessoas colectivas

O artigo 10º submete a uma condição as sanções contra pessoas colectivas consideradas responsáveis pelas infracções referidas nos artigos 3º, 4º e 5º. Estas sanções devem ser efectivas, proporcionadas e dissuasivas, sendo obrigatória no mínimo a imposição de multas de carácter penal ou não penal. São também indicadas outras sanções normalmente aplicáveis às pessoas colectivas.

Artigo 11º - Competência

Tendo em consideração a dimensão internacional das infracções que consistem em ataques contra sistemas de informação, só é possível uma resposta jurídica eficaz a estas infracções se as disposições processuais em matéria de competência e de extradição forem claras e ambiciosas a nível da União Europeia, a fim de evitar que os autores das infracções fiquem impunes.

O nº 1 estabelece uma série de critérios para a atribuição de competência às autoridades judiciárias nacionais tendo em vista um procedimento penal e a investigação de casos que envolvam infracções referidas na presente decisão-quadro. Um Estado-Membro estabelece a sua competência em três situações:

a) Se a infracção for praticada em todo ou em parte do seu território, independentemente do estatuto da pessoa colectiva ou da nacionalidade da pessoa singular implicada (princípio da territorialidade);

b) Se o autor da infracção for um nacional desse Estado-Membro (princípio da personalidade activa) e se o acto praticado afectar particulares ou grupos desse Estado-Membro. Incumbe aos Estados-Membros processar os seus próprios nacionais que são os autores de infracções praticadas no estrangeiro quando não está prevista a extradição;

c) Se a infracção for praticada em benefício de uma pessoa colectiva estabelecida no território desse Estado-Membro.

O nº 2 tem por objectivo garantir que aquando do estabelecimento da sua competência sobre as infracções abrangidas pelo princípio da territorialidade em conformidade com o disposto na alínea a) do nº 1, cada Estado-Membro deve assegurar que a mesma seja aplicável aos casos em que:

a) O autor da infracção praticou o acto quando se encontrava fisicamente presente no território desse Estado-Membro, quer a infracção vise ou não um sistema de informação situado no seu território. Por exemplo, uma pessoa obtém o acesso de forma ilícita a um sistema de informação de um país terceiro a partir do território desse Estado-Membro ("hacking"); ou

b) A infracção foi praticada contra um sistema de informação situado no território desse Estado-Membro, quer o infractor pratique ou não a infracção encontrando-se

fisicamente presente nesse território. Pode tratar-se, por exemplo, de uma pessoa que obtém ilegalmente acesso ao um sistema de informação situado no território do Estado-Membro a partir do território de um país terceiro ("hacking").

Tendo em conta que nem todas as ordens jurídicas dos Estados-Membros reconhecem uma competência extraterritorial relativamente a todos os tipos de infracções penais, o nº 3 permite-lhes não aplicar as normas de competência estabelecidas no nº 1 no que diz respeito às situações abrangidas pelas alíneas b) e c) do nº 1.

O n° 4 impõe que cada Estado-Membro tome as medidas necessárias para estabelecer igualmente a sua competência em relação às infracções referidas nos artigos 3° a 5°, 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.

O n° 5 abrange os casos de conflitos de competências jurisdicionais e tem por objectivo assegurar a plena cooperação entre Estados-Membros a fim de centralizar, se possível, os processos num único Estado-Membro. Para este efeito, recorda-se que 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. Incluem-se, neste caso, a Eurojust e a Rede Judiciária Europeia.

O nº 6 estabelece que os Estados-Membros devem informar o Secretariado-Geral do Conselho e a Comissão sempre que decidam aplicar o disposto no nº 3.

Artigo 12º – Intercâmbio de informações

O objectivo do artigo 12º consiste em facilitar o intercâmbio de informações através da designação de pontos de contacto operacionais, aspecto muito importante para efeitos de uma cooperação policial efectiva. Em especial, a necessidade de que o conjunto dos Estados-Membros adira à rede de pontos de contacto do G8 foi reconhecida pelo Conselho Justiça e Assuntos Internos, de 19 de Março de 1998, e mais recentemente quando adoptou uma recomendação do Conselho relativa a um serviço de 24 horas por dia de combate ao crime de alta tecnologia[36].

Artigo 13º - Aplicação

O artigo 13º diz respeito à aplicação e ao acompanhamento da presente decisão-quadro.

Os Estados-Membros devem tomar as medidas necessárias para dar cumprimento à presente decisão-quadro o mais tardar até 31 de Dezembro de 2003.

Os Estados-Membros devem transmitir, até essa data, ao Secretariado-Geral do Conselho e à Comissão as disposições de transposição para o direito nacional das obrigações que lhes são impostas por força da presente decisão-quadro. O Conselho avaliará, no prazo de um ano, com base nas informações comunicadas e num relatório escrito da Comissão, a medida em que os Estados-Membros cumpriram as obrigações impostas pela presente decisão-quadro.

---

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

Artigo 14º – Entrada em vigor

O artigo 14º estabelece que a presente decisão-quadro entrará em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial das Comunidades Europeias*.

2002/0086 (CNS)

Proposta de

DECISÃO-QUADRO DO CONSELHO

relativa a ataques contra os sistemas de informação

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia e, nomeadamente, o artigo 29º, o n° 1, alínea a), do artigo 30º, o artigo 31º e o nº 2, alínea b), do artigo 34º,

Tendo em conta a proposta da Comissão[1],

Tendo em conta o parecer do Parlamento Europeu[2],

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 eEurope, na Comunicação da Comissão intitulada "Segurança das redes e da informação: Proposta de abordagem de uma política europeia"[3] 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[4].

(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 judiciários 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,

---

1 JO C ... p.
2 JO C ... p.
3 COM (2001) 298.
4 [2001/2098 (INI)].

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 Amesterdão relativas à criação de um espaço de liberdade, de segurança e de justiça[5], 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[6], e a resolução do Parlamento Europeu de 19 de Maio de 2000[7], 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[8].

(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.

(8) A Decisão-quadro relativa ao mandado de captura europeu[9], 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[10], 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.

---

5 JO C 19 23.1.1999.
6 COM (2001) 278 final.
7 A5-0127/2000.
8 COM (2000) 890.
9 JO C , p. .
10 JO C , p. .

(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 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[11].

(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 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

---

11 JO L 351 de 29.12.1998, p. 1.

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° do Tratado da UE e previsto no artigo 5° 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 1º

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.

Artigo 2º

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 3º

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 4º

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 5º

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 3º e 4º sejam punidas como infracção penal.

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

Artigo 6º

Sanções

1. Os Estados-Membros assegurarão que as infracções referidas nos artigos 3º, 4° e 5º 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 7º

Circunstâncias agravantes

1. Os Estados-Membros assegurarão que as infracções referidas nos artigos 3°, 4° e 5° 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° e 4° sejam puníveis com uma pena privativa de liberdade superior às penas previstas ao abrigo do artigo 6°, se o infractor tiver sido condenado por essa infracção mediante sentença transitada em julgado num dos Estados-Membros.

Artigo 8º

Circunstâncias especiais

Não obstante o disposto nos artigos 6° e 7°, 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 9º

Responsabilidade das pessoas colectivas

1. Os Estados-Membros assegurarão que as pessoas colectivas possam ser consideradas responsáveis pelos actos referidos nos artigos 3º, 4º e 5º, 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 nº 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 nº 1, tiver possibilitado a prática das infracções referidas nos artigos 3º, 4º e 5º, em benefício dessa pessoa colectiva, por uma pessoa sob a sua autoridade.

3. A responsabilidade de uma pessoa colectiva nos termos do nº 1 e n° 2 não exclui o procedimento penal contra as pessoas singulares que praticarem as infracções ou os actos referidos nos artigos 3º, 4º e 5º.

Artigo 10º

Sanções aplicáveis às pessoas colectivas

1. Os Estados-Membros assegurarão que uma pessoa colectiva declarada responsável por força do nº 1 do artigo 9º 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 judiciárias de dissolução.

2. Os Estados-Membros assegurarão que uma pessoa colectiva declarada responsável por força do nº 2 do artigo 9º seja passível de sanções ou medidas efectivas, proporcionadas e dissuasivas.

Artigo 11º

Competência

1. Cada Estado-Membro determinará a sua competência relativamente às infracções referidas nos artigos 3º, 4º e 5º, 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 nº 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 nº 1.

4. Cada Estado-Membro tomará as medidas necessárias para estabelecer a sua competência em relação às infracções referidas nos artigos 3° a 5°, 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° 3, indicando, se for caso disso, os casos ou as circunstâncias especiais em que a decisão é aplicável.

Artigo 12º

Intercâmbio de informações

1. Para efeitos do intercâmbio de informações relativas às infracções referidas nos artigos 3º, 4° e 5º, e em conformidade com as normas em matéria de protecção de dados, os Estados-Membros assegurarão a designação de pontos de contacto operacionais disponíveis vinte e quatro 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 13º

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 14º

Entrada em vigor

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

Feito em Bruxelas,

Pelo Conselho
O Presidente