COMISSÃO EUROPEIA

Bruxelas, 30.9.2010
COM(2010) 517 final

2010/0273 (COD)

Proposta de

DIRECTIVA DO PARLAMENTO EUROPEU E DO CONSELHO

relativa a ataques contra os sistemas de informação e que revoga a Decisão-Quadro 2005/222/JAI do Conselho

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

EXPOSIÇÃO DE MOTIVOS

1. JUSTIFICAÇÃO E OBJECTIVOS DA PROPOSTA

A presente proposta tem como objectivo substituir a Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação[1]. Tal como indicado nos seus considerandos, a Decisão-Quadro visava 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. Introduziu legislação da UE para reprimir infracções como o acesso ilegal aos sistemas de informação, a interferência ilegal no sistema e a interferência ilegal nos dados, bem como disposições específicas relativas à responsabilidade das pessoas colectivas, à competência e ao intercâmbio de informações. Os Estados-Membros foram instados a adoptar as medidas necessárias para dar cumprimento às disposições da Decisão-Quadro até 16 de Março de 2007.

Em 14 de Julho de 2008, a Comissão publicou um relatório sobre a aplicação da Decisão-Quadro[2]. Nas suas conclusões, o relatório assinalou que tinham sido registados progressos consideráveis na maioria dos Estados-Membros e que o nível de transposição era considerado razoável, mas que alguns Estados-Membros não tinham ainda procedido à transposição. Mais à frente, o relatório afirmou que «recentes ataques ocorridos na Europa desde a adopção da DQ vieram chamar a atenção para várias ameaças emergentes, em especial a ocorrência de ataques massivos simultâneos contra sistemas de informação e o aumento da utilização das chamadas *botnets* para fins criminosos». Estes ataques não estavam no centro das atenções aquando da adopção da Decisão-Quadro. Em resposta a esta evolução, a Comissão ponderará a adopção de medidas destinadas a conceber respostas mais adaptadas à ameaça (ver a próxima secção para a explicação do que é um *botnet*).

A importância da adopção de outras medidas para intensificar a luta contra a cibercriminalidade foi sublinhada pelo Programa da Haia de 2004 relativo ao reforço da liberdade, da segurança e da justiça na União Europeia e pelo Programa de Estocolmo de 2009 e respectivo plano de acção[3]. Além disso, a Agenda Digital para a Europa[4] recentemente apresentada, que constitui a primeira iniciativa emblemática adoptada no âmbito da Estratégia «Europa 2020», reconheceu a necessidade de fazer face ao desenvolvimento de novas formas de criminalidade a nível europeu, nomeadamente a cibercriminalidade. Neste domínio de acção, em que a confiança e a segurança são cruciais, a Comissão está empenhada em adoptar medidas para combater os ciberataques contra os sistemas de informação.

A nível internacional, a Convenção do Conselho da Europa sobre a Criminalidade Informática («Convenção Cibercriminalidade»), assinada em 23 de Novembro de 2001, é considerada como a norma internacional mais completa até ao presente, uma vez que proporciona um

---

1 JO L 69 de 16.3.2005, p. 68.

2 Relatório da Comissão ao Conselho apresentado nos termos do artigo 12.º da Decisão-Quadro do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação - COM (2008) 0448 final.

3 JO C 198 de 12.8.2005, JO C 115 de 4.5.2010, COM (2010) 171 de 20.4.2010.

4 Comunicação da Comissão, COM (2010) 245 de 19.5.2010.

quadro global e coerente que cobre os vários aspectos da cibercriminalidade[5]. Até à data, a Convenção foi assinada pelos 27 Estados-Membros, mas só 15 deles a ratificaram[6]. A Convenção entrou em vigor em 1 de Julho de 2004. A UE não é signatária da Convenção. Dada a importância deste instrumento, a Comissão encoraja vivamente os restantes Estados-Membros da UE a ratificarem a Convenção o mais rapidamente possível.

- **Contexto geral**

A principal causa da cibercriminalidade é a vulnerabilidade resultante de vários factores. Uma resposta insuficiente dos mecanismos de aplicação da lei contribui para a prevalência destes fenómenos e agrava as dificuldades, já que certos tipos de crimes têm carácter transfronteiriço. As denúncias relativas a este tipo de crime são muitas vezes inadequadas, em parte porque alguns crimes não são detectados e em parte porque as vítimas (operadores económicos e empresas) não os denunciam por temerem que a exposição pública das suas vulnerabilidades afecte a sua reputação e as perspectivas comerciais futuras.

Além disso, as diferenças entre as legislações e procedimentos penais nacionais podem dar origem a diferenças a nível da investigação e das acções penais, conduzindo a discrepâncias no tratamento dado a estes crimes. A evolução no domínio das tecnologias da informação exacerbam estes problemas, facilitando a produção e distribuição de instrumentos («malware» e «botnets») e proporcionando ao mesmo tempo anonimato aos infractores e dispersando a responsabilidade por várias jurisdições. Dadas as dificuldades em levar a cabo uma acção penal, a criminalidade organizada consegue obter lucros consideráveis com riscos reduzidos.

A presente proposta tem em conta os novos métodos utilizados para cometer cibercrimes, nomeadamente o recurso aos «botnets». O termo «botnet» designa uma rede de computadores que foram infectados por *software* maligno (vírus informáticos). Esta rede de computadores «sequestrados» («zombies») pode ser activada para executar acções específicas, como atacar sistemas de informação (ciberataques). Estes «zombies» podem ser controlados – frequentemente sem o conhecimento dos utilizadores dos computadores «sequestrados» – por outro computador, igualmente conhecido como «centro de comando e de controlo». As pessoas que controlam este centro fazem parte dos infractores, já que utilizam os computadores «sequestrados» para lançar ataques contra os sistemas de informação. É muito difícil localizar os autores da infracção, dado que os computadores que formam o «botnet» e realizam o ataque podem encontrar-se num local diferente daquele em que se encontra o infractor.

Os ataques perpetrados por um «botnet» são frequentemente lançados em larga escala. Os ataques em larga escala são aqueles que podem ser realizados utilizando instrumentos que afectem um número significativo de sistemas de informação (computadores), ou os ataques que causam danos consideráveis, por exemplo em termos de perturbação dos serviços do sistema, custos financeiros, perda de dados pessoais, etc. Os danos causados pelos ataques em larga escala têm um impacto significativo no funcionamento do próprio objectivo e/ou afectam o seu ambiente de trabalho. Neste contexto, considera-se que um grande «botnet» tem capacidade para causar danos graves. É difícil definir os «botnets» em termos de dimensão, mas estima-se que os maiores «botnets» registados têm entre 40 000 e 100 000 conexões (ou

---

5 Convenção do Conselho da Europa sobre a Cibercriminalidade Informática, Budapeste, 23.11.2001, STCE-185.

6 Para uma perspectiva geral das ratificações da Convenção (STCE-185), consultar: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

seja, computadores infectados) por período de 24 horas[7].

- **Disposições em vigor no domínio da proposta**

A nível da UE, a Decisão-Quadro introduz um nível mínimo de aproximação das legislações dos Estados-Membros com vista a criminalizar vários cibercrimes, designadamente o acesso ilegal aos sistemas de informação, a interferência ilegal no sistema, a interferência ilegal nos dados e a instigação, cumplicidade e tentativa.

Embora, de um modo geral, as disposições da Decisão-Quadro tenham sido transpostas pelos Estados-Membros, o texto tem algumas lacunas imputáveis à tendência registada na dimensão e no número de infracções (ciberataques). Aproxima as legislações apenas relativamente a um número limitado de infracções, mas não permite fazer plenamente face à ameaça potencial que os ataques em larga escala representam para a sociedade. Também não tem devidamente em conta a gravidade das infracções e as sanções que lhes são aplicadas.

Outras iniciativas e programas da UE, em vigor ou previstos, tentam resolver os problemas relacionados com os ciberataques ou as questões como a segurança das redes e a protecção dos utilizadores da Internet. Incluem acções apoiadas pelos programas «Prevenir e combater a criminalidade»[8], «Justiça penal»[9] e «Para uma Internet mais Segura»[10] e pela iniciativa «Infra-estruturas críticas da informação»[11]. Para além da Decisão-Quadro, outro instrumento jurídico pertinente em vigor é a Decisão-Quadro 2004/68/JAI relativa à luta contra a exploração sexual de crianças e a pornografia infantil.

A nível administrativo, a prática da infecção de computadores para os transformar em «botnets» é já proibida ao abrigo das normas da UE relativas à protecção da privacidade e dos dados[12]. Os organismos administrativos nacionais, nomeadamente, já cooperam no âmbito da Rede de Contacto das Autoridades responsáveis pelo Combate ao *Spam*. Ao abrigo destas normas, os Estados-Membros são obrigados a proibir a intercepção de comunicações nas redes públicas de telecomunicações e nos serviços de comunicações electrónicas publicamente disponíveis sem o consentimento dos utilizadores em causa ou uma autorização legal.

A presente proposta está em conformidade com essas regras. Os Estados-Membros devem procurar melhorar a cooperação entre as autoridades administrativas e as autoridades responsáveis pela aplicação da lei nos casos passíveis de sanções de natureza administrativa e penal.

- **Coerência com outras políticas e objectivos da União**

Os objectivos são coerentes com as políticas da UE destinadas a combater a criminalidade organizada, aumentar a resiliência das redes informáticas e proteger as infra-estruturas críticas da informação e os dados. São igualmente coerentes com o programa «Para uma Internet mais

---

7 O número de conexões por 24 horas é a unidade de medida geralmente utilizada para calcular a dimensão dos «botnets».

8 Ver: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 Ver: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm

10 Ver: http://ec.europa.eu/information_society/activities/sip/index_en.htm

11 Ver: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12 Directiva relativa à privacidade e às comunicações electrónicas (JO L 201 de 31.7.2002), com a redacção que lhe foi dada pela Directiva 2009/136/CE (JO L 337 de 18.12.2009).

segura», concebido para promover uma utilização mais segura da Internet e das novas tecnologias em linha, bem como para combater os conteúdos ilegais.

A presente proposta foi objecto de uma análise aprofundada para garantir a plena compatibilidade das suas disposições com os direitos fundamentais, nomeadamente a protecção dos dados pessoais, a liberdade de expressão e informação, o direito a um tribunal imparcial, a presunção de inocência e os direitos da defesa, assim como com os princípios da legalidade e proporcionalidade das infracções e sanções penais.

2. CONSULTA DAS PARTES INTERESSADAS E AVALIAÇÃO DE IMPACTO

- **Consulta das partes interessadas**

Foi consultado um amplo leque de peritos neste domínio em várias reuniões consagradas a diferentes aspectos da luta contra a cibercriminalidade, incluindo o acompanhamento judicial (acção penal) destes crimes. Entre estes peritos contavam-se, nomeadamente, representantes dos governos dos Estados-Membros e do sector privado, juízes e magistrados do Ministério Público especializados, organizações internacionais, agências europeias e organismos especializados. Vários peritos e organizações enviaram posteriormente artigos e informações.

As principais conclusões da consulta são as seguintes:

– necessidade de intervenção da UE neste domínio;

– necessidade de criminalizar certas formas de infracções não incluídas na actual Decisão-Quadro, em especial as novas formas de ciberataques («botnets»);

– necessidade de eliminar os obstáculos às investigações e acções penais nos processos transfronteiras.

Os contributos recebidos durante a consulta foram tidos em consideração na avaliação de impacto.

Obtenção e utilização de competências especializadas

As competências externas foram obtidas durante várias reuniões com as partes interessadas.

Avaliação de impacto

Foram analisadas várias opções tendo em vista o cumprimento do objectivo.

- Opção n.º 1: *Statu quo*/Nenhuma nova acção da UE

Esta opção significa que a UE não tomará quaisquer outras medidas para combater este tipo específico de cibercriminalidade, ou seja, os ataques contra os sistemas de informação. As acções em curso devem ser prosseguidas, em especial os programas destinados a reforçar a protecção das infra-estruturas críticas da informação e a melhorar a cooperação entre os sectores público e privado face à cibercriminalidade.

- Opção n.º 2: Desenvolvimento de um programa com vista a intensificar os esforços para combater os ataques contra os sistemas de informação através de medidas não legislativas

Paralelamente ao programa de protecção das infra-estruturas críticas da informação, as medidas não legislativas centrar-se-iam na repressão transfronteiras e na cooperação entre os sectores público e privado. Estes instrumentos jurídicos não vinculativos devem procurar promover outras acções coordenadas a nível da UE, nomeadamente o reforço da rede de pontos de contacto disponíveis 24 horas por dia e 7 dias por semana dos organismos responsáveis pela aplicação da lei; a criação de uma rede da UE de pontos de contacto dos sectores público e privado que reúnam peritos em cibercriminalidade e organismos responsáveis pela aplicação da lei; a elaboração de um modelo de acordo da UE sobre os níveis de serviço com vista à cooperação policial com os operadores do sector privado; e o apoio à organização de programas de formação sobre a investigação da cibercriminalidade destinados aos organismos responsáveis pela aplicação da lei.

- Opção n.º 3: Actualização orientada das disposições da Decisão-Quadro (nova directiva para substituir a actual Decisão-Quadro) para responder à ameaça de ataques em larga escala contra os sistemas de informação («botnets») e, quando perpetrados mediante a dissimulação da verdadeira identidade do autor e causando prejuízo ao titular legítimo da identidade, para aumentar a eficácia dos pontos de contacto responsáveis pela aplicação da lei dos Estados-Membros e fazer face à falta de dados estatísticos sobre os ciberataques.

Esta opção prevê a introdução de legislação específica orientada (ou seja, limitada) para impedir os ataques em larga escala contra os sistemas de informação. Tal legislação reforçada seria acompanhada de medidas não legislativas destinadas a reforçar a cooperação operacional transfronteiriça contra estes ataques, o que facilitaria a aplicação das medidas legislativas. Estas medidas teriam como objectivo melhorar a preparação, a segurança e a resiliência das infra-estruturas críticas da informação e o intercâmbio de boas práticas.

- Opção n.º 4: Adopção de legislação global da UE contra a cibercriminalidade

Esta opção implicaria uma nova legislação abrangente da UE. Para além da introdução de instrumentos legislativos não vinculativos prevista na opção 2 e da actualização referida na opção 3, esta solução abordaria igualmente outros problemas jurídicos relacionados com a utilização da Internet. Tais medidas abrangeriam não só os ataques contra os sistemas de informação, mas também questões como a cibercriminalidade financeira, os conteúdos ilegais na Internet e a recolha/armazenagem/transferência de provas electrónicas e preveriam regras de competência mais pormenorizadas. A legislação seria aplicável paralelamente à Convenção do Conselho da Europa sobre a Criminalidade Informática e incluiria as medidas não legislativas de acompanhamento acima mencionadas.

- Opção n.º 5: Actualização da Convenção do Conselho da Europa sobre a Criminalidade Informática

Esta opção exigiria a renegociação de uma parte substancial da actual Convenção, um processo moroso e portanto incompatível com o calendário de acção proposto na avaliação de impacto. A nível internacional não parece haver vontade de renegociar a Convenção. Por conseguinte, a sua actualização não pode ser considerada uma opção viável, já que ultrapassaria o prazo previsto para a acção.

Opção preferida: combinação de medidas não legislativas (opção 2) com uma actualização orientada da Decisão-Quadro (opção 3)

Na sequência da análise dos impactos económicos, sociais e a nível dos direitos fundamentais, as opções 2 e 3 representam a melhor abordagem para resolver o problema e atingir os objectivos da proposta.

Ao elaborar a presente proposta, a Comissão realizou uma avaliação de impacto.

3. ELEMENTOS JURÍDICOS DA PROPOSTA

- **Síntese da acção proposta**

Embora revogue a Decisão-Quadro 2005/222/JAI, a directiva manterá as suas disposições actuais e incluirá os seguintes novos elementos:

– No domínio do direito penal material em geral, a directiva:

A. Sanciona a produção, venda, aquisição para utilização, importação, distribuição ou outra forma de disponibilizar os dispositivos/instrumentos utilizados para cometer as infracções.

B. Prevê circunstâncias agravantes:

- os ataques em grande escala – serão combatidos os «botnets» ou instrumentos semelhantes mediante a introdução de uma nova circunstância agravante: o acto de criar um «botnet» ou um instrumento semelhante constitui um factor agravante quando são cometidos os crimes enumerados na Decisão-Quadro em vigor;

- quando tais ataques são perpetrados mediante a dissimulação da identidade real do autor e causando prejuízos ao titular legítimo da identidade. Todas estas disposições devem estar em conformidade com os princípios da legalidade e da proporcionalidade das infracções e das sanções penais e ser coerentes com a legislação em vigor relativa à protecção dos dados pessoais[13].

C. Introduz a «intercepção ilegal» como infracção.

D. Introduz medidas para melhorar a cooperação em matéria de justiça penal a nível europeu mediante o reforço da estrutura existente de pontos de contacto disponíveis 24 horas por dia e 7 dias por semana[14]:

- é proposta a obrigação de dar resposta a um pedido de assistência dos pontos de contacto operacionais (prevista no artigo 14.° da directiva) dentro de um certo prazo. A Convenção sobre a Criminalidade Informática não especifica uma disposição vinculativa deste tipo. O objectivo desta medida é assegurar que os

[13] Como a Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12.7.2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas) (JO L 201 de 31.7.2002, p. 37) (actualmente em revisão) e como a Directiva 95/46/CE relativa à protecção de dados.

[14] Introduzida pela Convenção, e DQ 2005/222/JAI relativa a ataques contra os sistemas de informação.

pontos de contacto indiquem, num determinado prazo, se podem responder ao pedido de assistência e qual o prazo em que o ponto de contacto requerente pode esperar a solução para o problema apresentado. O conteúdo concreto das soluções não é especificado.

E. Responde à necessidade de dispor de dados estatísticos sobre a cibercriminalidade, tornando obrigatória para os Estados-Membros a criação de um sistema adequado para o registo, produção e disponibilização de dados estatísticos sobre as infracções referidas na Decisão-Quadro em vigor e sobre a nova infracção «intercepção ilegal».

A directiva contém, nas definições das infracções penais enumeradas nos artigos 3.º, 4.º e 5.º (acesso ilegal aos sistemas de informação, interferência ilegal no sistema e interferência ilegal nos dados), uma disposição que permite unicamente a criminalização dos «casos que tenham alguma gravidade» no processo de transposição da directiva para o direito nacional. Este elemento de flexibilidade destina-se a permitir aos Estados-Membros não abranger os casos que, *in abstracto*, seriam abrangidos pela definição de base, mas que se considere não prejudicarem o interesse jurídico protegido, por exemplo os actos cometidos por jovens ao tentarem provar a sua perícia no domínio das tecnologias da informação. Esta possibilidade de limitar o âmbito da criminalização não deverá no entanto levar à introdução de novos elementos constitutivos das infracções para além dos já previstos na directiva, já que tal conduziria a uma situação em que só seriam abrangidas as infracções cometidas com circunstâncias agravantes. Aquando da transposição, os Estados-Membros devem abster-se de acrescentar novos elementos constitutivos às infracções de base, como por exemplo a intenção específica de obter produtos ilegais do crime ou a presença de um efeito específico, como causar danos consideráveis.

- **Base jurídica**

Artigo 83.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia[15].

- **Princípio da subsidiariedade**

O princípio da subsidiariedade aplica-se às acções da União Europeia. Os objectivos da proposta não podem ser suficientemente realizados pelos Estados-Membros pelas seguintes razões:

A cibercriminalidade e, mais especificamente, os ataques contra os sistemas de informação têm uma dimensão transfronteiriça considerável, que é mais óbvia nos ataques em larga escala, já que os elementos de ligação de um ataque estão frequentemente situados em diferentes locais e em países diferentes. Tal exige uma acção da UE, nomeadamente para não se deixar ultrapassar pela tendência actual que consiste em lançar ataques em larga escala a nível europeu e mundial. As conclusões do Conselho de Novembro de 2008[16] apelaram a uma acção a nível da UE e à actualização da Decisão-Quadro 2005/222/JAI, dado que o objectivo de proteger eficazmente os cidadãos da cibercriminalidade não pode ser suficientemente alcançado pelos Estados-Membros.

---

15 JO C 83 de 30.3.2010, p. 49.

16 «Estratégia de trabalho concertada e medidas concretas contra o cibercrime», 2987.ª reunião do Conselho JUSTIÇA E ASSUNTOS INTERNOS, Bruxelas, 27 e 28 de Novembro de 2008.

Os objectivos da proposta podem ser melhor realizados a nível da União pelas razões que se seguem.

A proposta prosseguirá a aproximação do direito penal material dos vários Estados-Membros e das suas normas processuais, o que terá um impacto positivo na luta contra estas infracções. Em primeiro lugar, é uma forma de impedir os infractores de se instalarem nos Estados-Membros cuja legislação aplicável aos ciberataques é mais clemente. Em segundo lugar, o facto de existirem definições comuns possibilita o intercâmbio de informações e a recolha e comparação dos dados pertinentes. Em terceiro lugar, a eficácia das medidas de prevenção na UE e a cooperação internacional também são reforçadas.

Por conseguinte, a proposta respeita o princípio da subsidiariedade.

- **Princípio da proporcionalidade**

A proposta respeita o princípio da proporcionalidade pela seguinte razão:

A presente directiva limita-se ao mínimo indispensável para alcançar esses objectivos ao nível europeu e não excede o necessário para esse efeito, tendo em conta
a necessidade de dispor de legislação penal fiável.

- **Escolha dos instrumentos**

Instrumento proposto: directiva.

O recurso a outros meios não seria apropriado pelo seguinte motivo:

A base jurídica requer uma directiva.

Determinadas medidas não legislativas e a auto-regulação contribuiriam para melhorar a situação em certos domínios em que a aplicação é crucial. No entanto, noutros domínios em que é essencial adoptar nova legislação os benefícios seriam modestos.

4. INCIDÊNCIA ORÇAMENTAL

A incidência da proposta no orçamento da União é reduzida. Mais de 90 % dos custos, estimados em 5 913 000 EUR, seriam suportados pelos Estados-Membros e existe a possibilidade de solicitar um financiamento da UE para reduzir os mesmos.

5. INFORMAÇÕES COMPLEMENTARES

- **Revogação da legislação em vigor**

A adopção da proposta conduzirá à revogação da legislação em vigor.

- **Âmbito de aplicação territorial**

Os Estados-Membros são os destinatários da presente directiva, em conformidade com os Tratados.

2010/0273 (COD)

Proposta de

DIRECTIVA DO PARLAMENTO EUROPEU E DO CONSELHO

relativa a ataques contra os sistemas de informação e que revoga a Decisão-Quadro 2005/222/JAI do Conselho

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente

o artigo 83.º, n.º 1,

Tendo em conta a proposta da Comissão Europeia[17],

Após transmissão do projecto aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu,

Tendo em conta o parecer do Comité das Regiões,

Deliberando nos termos do processo legislativo ordinário,

Considerando o seguinte:

(1) A presente directiva tem como objectivo aproximar as disposições em matéria de direito penal dos Estados-Membros relativas aos ataques contra os sistemas de informação e melhorar a cooperação entre as autoridades judiciais e outras autoridades competentes, nomeadamente a polícia e outros serviços especializados dos Estados-Membros responsáveis pela aplicação da lei.

(2) Os ataques contra os sistemas de informação, em especial os perpetrados pela criminalidade organizada, constituem uma ameaça crescente e a eventualidade de ataques terroristas ou de natureza política contra os sistemas de informação que fazem parte da infra-estrutura crítica dos Estados-Membros e da União suscita uma preocupação cada vez maior. Esta ameaça pode pôr em causa a concretização de uma sociedade da informação mais segura, bem como a realização do espaço de liberdade, de segurança e de justiça, exigindo, portanto, uma resposta ao nível da União Europeia.

(3) Existem provas de uma tendência para perpetrar ataques cada vez mais perigosos e recorrentes em larga escala contra sistemas de informação cruciais para os Estados ou para certas funções específicas do sector público ou privado. Esta tendência é acompanhada pelo desenvolvimento de instrumentos cada vez mais sofisticados, que podem ser utilizados pelos criminosos para lançar ciberataques de vários tipos.

---

[17] JO C […] de […], p. […].

(4) É importante adoptar definições comuns neste domínio, nomeadamente no que diz respeito aos sistemas de informação e aos dados informáticos, de modo a assegurar a coerência da aplicação da presente directiva nos Estados-Membros.

(5) É necessário adoptar uma abordagem comum sobre os elementos constitutivos de infracções penais, introduzindo as infracções comuns do acesso ilegal aos sistemas de informação, interferência ilegal nos sistemas, interferência ilegal nos dados e intercepção ilegal.

(6) Os Estados-Membros devem prever sanções para os ataques contra os sistemas de informação. As sanções previstas devem ser efectivas, proporcionadas e dissuasivas.

(7) Convém prever sanções mais severas nos casos em que os ataques contra um sistema de informação forem perpetrados por organizações criminosas, tal como definidas na Decisão-Quadro 2008/841/JAI do Conselho, de 24 de Outubro de 2008, relativa à luta contra a criminalidade organizada[18], quando os ataques forem conduzidos em larga escala, ou quando, para cometer uma infracção, o seu autor dissimular a sua identidade real causando prejuízos ao titular legítimo da identidade. É igualmente oportuno prever sanções mais severas quando os ataques tiverem causado danos graves ou lesado interesses essenciais.

(8) Nas suas conclusões de 27 e 28 de Novembro de 2008, o Conselho convidou os Estados-Membros e a Comissão a desenvolverem uma nova estratégia, tendo em conta o conteúdo da Convenção do Conselho da Europa sobre a Criminalidade Informática de 2001. Esta Convenção é o quadro jurídico de referência do combate à cibercriminalidade, incluindo os ataques contra os sistemas de informação. A presente directiva baseia-se nessa Convenção.

(9) Tendo em conta as diferentes formas como os ataques podem ser realizados e a rápida evolução do *hardware* e do *software*, a presente directiva faz referência a «instrumentos» que podem ser utilizados para cometer as infracções nela enumeradas. Por «instrumentos» entende-se, por exemplo, *software* maligno, incluindo «botnets», utilizado para cometer ciberataques.

(10) A presente directiva não pretende impor responsabilidade penal quando as infracções forem cometidas sem objectivos criminosos, por exemplo para efectuar testes autorizados ou proteger sistemas informáticos.

(11) A presente directiva reforça a importância das redes, como a rede do G8 ou do Conselho da Europa de pontos de contacto disponíveis 24 horas por dia e 7 dias por semana para trocar informações, a fim de prestar assistência imediata no âmbito de inquéritos ou procedimentos relativos a infracções penais ligadas a sistemas e dados informáticos, ou para recolher provas electrónicas de uma infracção penal. Dada a velocidade com que os ataques em larga escala podem ser realizados, os Estados-Membros devem poder responder prontamente aos pedidos urgentes provenientes desta rede de pontos de contacto. A assistência solicitada deve consistir, nomeadamente, em facilitar ou executar directamente medidas como a prestação de aconselhamento técnico, a conservação de dados, a recolha de provas, a prestação de informações jurídicas e a localização de suspeitos.

---

[18] JO L 300 de 11.11.2008, p. 42.

(12) É necessário recolher dados sobre as infracções abrangidas pela presente directiva, a fim de dispor de uma imagem mais completa do problema a nível da União e contribuir assim para a formulação de respostas mais eficazes. Além disso, graças aos dados recolhidos, as agências especializadas, como a Europol e a Agência Europeia para a Segurança das Redes e da Informação, poderão avaliar melhor a extensão da cibercriminalidade e o nível de segurança das redes e da informação na Europa.

(13) As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros no domínio dos ataques contra os sistemas de informação podem entravar a luta contra a criminalidade organizada e o terrorismo e dificultar uma cooperação policial e judicial eficaz nesta área. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra estes sistemas tenham uma dimensão transfronteiriça, o que evidencia a necessidade urgente de adoptar medidas suplementares para harmonizar o direito penal neste domínio. Além disso, a coordenação da acção penal contra casos de ataques a sistemas de informação será facilitada com a adopção da Decisão-Quadro 2009/948/JAI do Conselho relativa à prevenção e resolução de conflitos de exercício de competência em processo penal.

(14) Atendendo a que os objectivos da presente directiva, 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 e melhorar e favorecer a cooperação judiciária suprimindo eventuais 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 adoptar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. A presente directiva não excede o necessário para atingir estes objectivos.

(15) O tratamento de dados pessoais no quadro da aplicação da presente directiva deve ser conforme com as regras estabelecidas na Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal[19] no que diz respeito às actividades de tratamento abrangidas pelo seu âmbito de aplicação e pelo Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados[20].

(16) A presente directiva respeita os direitos fundamentais e observa os princípios reconhecidos pela Carta dos Direitos Fundamentais da União Europeia, designadamente a protecção dos dados pessoais, a liberdade de expressão e de informação, o direito à acção e a um tribunal imparcial, a presunção de inocência e os direitos de defesa, bem como os princípios da legalidade e da proporcionalidade dos delitos e das penas. A presente directiva procura nomeadamente garantir o pleno respeito destes direitos e princípios e deve ser aplicada em conformidade.

(17) [Nos termos dos artigos 1.°, 2.°, 3.° e 4.° do Protocolo relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, de segurança e de justiça, anexo

---

19 JO L 350 de 30.12.2008, p. 60.

20 JO L 8 de 12.01.2001, p. 1.

ao Tratado sobre o Funcionamento da União Europeia, o Reino Unido e a Irlanda notificaram o desejo de participar na adopção e aplicação da presente directiva] OU [Sem prejuízo do disposto no artigo 4.º do Protocolo relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, de segurança e de justiça, o Reino Unido e a Irlanda não participam na adopção da presente directiva, não ficando por ela vinculados nem sujeitos à sua aplicação].

(18) Nos termos dos artigos 1.º e 2.º do Protocolo relativo à posição da Dinamarca, anexo ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participa na adopção da presente directiva, não ficando por ela vinculada nem sujeita à sua aplicação,

ADOPTARAM A PRESENTE DIRECTIVA:

Artigo 1.º
Objecto

A presente directiva define infracções penais no domínio de ataques contra os sistemas de informação e estabelece normas mínimas relativas às sanções aplicáveis a essas infracções. Visa também introduzir disposições comuns para prevenir tais ataques e melhorar a cooperação judicial europeia neste domínio.

Artigo 2.º
Definições

Para efeitos da presente directiva, entende-se por:

a) «Sistema de informação», qualquer dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, graças a um programa, o tratamento automático de dados informáticos, bem como de 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 que possam ser tratados 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;

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

Artigo 3.º

Acesso ilegal aos sistemas de informação

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 tenham alguma gravidade.

Artigo 4.º

Interferência ilegal no sistema

Os Estados-Membros devem 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 tenham alguma gravidade.

Artigo 5.º

Interferência ilegal nos dados

Os Estados-Membros devem 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 tenham alguma gravidade.

Artigo 6.º

Intercepção ilegal

Os Estados-Membros devem tomar as medidas necessárias para assegurar que a intercepção intencional e não autorizada, através de meios técnicos, de transmissões não públicas de dados informáticos, a partir de ou num sistema de informação, incluindo emissões electromagnéticas de um sistema de informação que comporte esses dados, seja punível como infracção penal.

Artigo 7.º

Instrumentos utilizados para cometer infracções

Os Estados-Membros devem tomar as medidas necessárias para assegurar que a produção, venda, aquisição para utilização, importação, posse, distribuição ou outra forma de disponibilizar os seguintes elementos seja punível como infracção penal quando cometida intencionalmente e sem autorização para os utilizar a fim de praticar qualquer das infracções referidas nos artigos 3.º a 6.º:

a) um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para cometer qualquer das infracções referidas nos artigos 3.° a 6.°;

b) uma palavra-passe, um código de acesso ou dados similares que permitam aceder à totalidade ou a parte de um sistema de informação.

Artigo 8.º

Instigação, auxílio, cumplicidade e tentativa

1. Os Estados-Membros devem assegurar que a instigação, o auxílio e a cumplicidade na prática de uma infracção referida nos artigos 3.º a 7.º sejam puníveis como infracções penais.

2. Os Estados-Membros devem assegurar que a tentativa de prática das infracções referidas nos artigos 3.º a 6.º seja punível como infracção penal.

Artigo 9.º

Sanções

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 3.º a 8.º sejam puníveis com sanções efectivas, proporcionadas e dissuasivas.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 3.º a 7.º sejam puníveis com uma pena máxima de prisão não inferior a dois anos.

Artigo 10.º

Circunstâncias agravantes

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 3.º a 7.º sejam puníveis com uma pena máxima de prisão não inferior a cinco anos, quando cometidas no âmbito de uma organização criminosa, tal como definida na Decisão-Quadro 2008/841/JAI.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 3.º a 6.º sejam puníveis com uma pena máxima de prisão não inferior a cinco anos, quando cometidas recorrendo a um instrumento concebido para lançar ataques que afectem um número significativo de sistemas de informação ou ataques que causem danos consideráveis, como perturbações de serviços do sistema, custos financeiros ou perda de dados pessoais.

3. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 3.º a 6.º sejam puníveis com uma pena máxima de prisão não inferior a cinco anos, quando cometidas mediante a dissimulação da identidade real do seu autor e causando prejuízos ao titular legítimo da identidade.

Artigo 11.º

Responsabilidade das pessoas colectivas

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as pessoas colectivas possam ser responsabilizadas pelas infracções referidas nos artigos 3.º a 8.º cometidas em seu benefício por qualquer pessoa, agindo a título individual ou como membro de um órgão da pessoa colectiva e que nela tenha uma posição proeminente, com base num dos seguintes elementos:

a) Poder de representação da pessoa colectiva;

b) Autoridade para tomar decisões em nome da pessoa colectiva;

c) Autoridade para exercer controlo dentro da pessoa colectiva.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as pessoas colectivas possam ser responsabilizadas sempre que a falta de supervisão ou de controlo por parte de uma pessoa referida no n.º 1 tenha tornado possível a prática, por uma pessoa que lhe seja subordinada, das infracções referidas nos artigos 3.º a 8.º em benefício dessa pessoa colectiva.

3. A responsabilidade das pessoas colectivas por força dos n.os 1 e 2 não exclui a acção penal contra as pessoas singulares que sejam autoras ou cúmplices de qualquer das infracções referidas nos artigos 3.º a 8.º

Artigo 12.º
Sanções aplicáveis às pessoas colectivas

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do artigo 11.º, n.º 1, seja passível de sanções efectivas, proporcionadas e dissuasivas, incluindo multas ou coimas e, eventualmente, outras sanções, designadamente:

a) Exclusão de benefícios ou auxílios públicos;

b) Proibição temporária ou permanente de exercer actividades comerciais;

c) Colocação sob controlo judicial;

d) Liquidação judicial;

e) Encerramento temporário ou definitivo dos estabelecimentos utilizados para a prática do crime.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do artigo 11.º, n.º 2, seja passível de sanções ou medidas efectivas, proporcionadas e dissuasivas.

Artigo 13.º
Competência

1. Os Estados-Membros devem determinar a sua própria competência relativamente às infracções referidas nos artigos 3.º a 8.º, sempre que a infracção tenha sido cometida:

a) Total ou parcialmente no território do Estado-Membro em causa; ou

b) Por um nacional seu ou uma pessoa que tenha a sua residência habitual no território do Estado-Membro em causa; ou

c) Em benefício de uma pessoa colectiva cuja sede se situe no território do Estado-Membro em causa.

2. Ao definirem a sua competência em conformidade com o n.º 1, alínea a), os Estados-Membros devem assegurar que sejam incluídos os casos em que:

a) O autor cometeu a infracção quando se encontrava fisicamente presente no território do Estado-Membro em causa, independentemente de a infracção visar ou não um sistema de informação situado no seu território; ou

b) A infracção foi cometida contra um sistema de informação situado no território do Estado-Membro em causa, independentemente de o seu autor se encontrar ou não fisicamente presente no seu território;

Artigo 14.º
Intercâmbio de informações

1. Para efeitos do intercâmbio de informações relativas às infracções referidas nos artigos 3.º a 8.º e em conformidade com as normas em matéria de protecção de dados, os Estados-Membros devem recorrer à rede existente de pontos de contacto operacionais, disponível 24 horas por dia e 7 dias por semana. Os Estados-Membros devem também assegurar que dispõem de procedimentos que lhes permitam responder aos pedidos urgentes no prazo máximo de oito horas. A resposta deve pelo menos indicar se, de que forma e quando será atendido o pedido de ajuda.

2. Os Estados-Membros devem comunicar à Comissão o nome do seu ponto de contacto designado para efeitos do intercâmbio de informações sobre as infracções referidas nos artigos 3.º a 8.º. A Comissão deve transmitir essas informações aos restantes Estados-Membros.

Artigo 15.º
Acompanhamento e estatísticas

1. Os Estados-Membros devem assegurar a existência de um sistema para o registo, produção e disponibilização de dados estatísticos sobre as infracções referidas nos artigos 3.° a 8.°.

2. As estatísticas referidas no n.º 1 devem cobrir, no mínimo, o número de infracções referidas nos artigos 3.º a 8.º comunicadas aos Estados-Membros e o seguimento dado a estas denúncias, bem como indicar, anualmente, o número de casos denunciados objecto de investigação, o número de pessoas objecto de procedimento penal e o número de pessoas condenadas pelas infracções referidas nos artigos 3.º a 8.º.

3. Os Estados-Membros devem transmitir à Comissão os dados recolhidos nos termos do presente artigo. Devem também assegurar a publicação de uma revisão consolidada destes relatórios estatísticos.

Artigo 16.º

Revogação da Decisão-Quadro 2005/222/JAI

É revogada a Decisão-Quadro 2005/222/JAI, sem prejuízo das obrigações dos Estados-Membros relativas aos prazos de transposição para o direito nacional.

As referências feitas à decisão-quadro revogada devem entender-se como sendo feitas à presente directiva.

Artigo 17.º

Transposição

1. Os Estados-Membros devem adoptar as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente directiva o mais tardar até [dois anos a contar da adopção]. Os Estados-Membros devem comunicar imediatamente à Comissão o texto dessas disposições, bem como um quadro de correspondência entre as mesmas e a presente directiva. Quando os Estados-Membros adoptarem essas disposições, estas devem incluir uma referência à presente directiva ou ser acompanhadas dessa referência aquando da sua publicação oficial. As modalidades dessa referência devem ser estabelecidas pelos Estados-Membros.

2. Os Estados-Membros devem comunicar à Comissão o texto das principais disposições de direito nacional que adoptarem no domínio abrangido pela presente directiva.

Artigo 18.º

Relatórios

1. A Comissão deve apresentar ao Parlamento Europeu e ao Conselho até [QUATRO ANOS A CONTAR DA ADOPÇÃO] e, em seguida, de três em três anos, um relatório relativo à aplicação da presente directiva nos Estados-Membros, acompanhado de eventuais propostas consideradas necessárias.

2. Os Estados-Membros devem transmitir à Comissão todas as informações necessárias para a elaboração do relatório referido no n.º 1. As informações devem incluir uma descrição pormenorizada das medidas legislativas e não legislativas adoptadas para aplicar a presente directiva.

Artigo 19.º

Entrada em vigor

A presente directiva entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Artigo 20.º
Destinatários

Os Estados-Membros são os destinatários da presente directiva, em conformidade com os Tratados.

Feito em Bruxelas,

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*