DIRETIVA 2013/40/UE DO PARLAMENTO EUROPEU E DO CONSELHO

de 12 de agosto de 2013

relativa a ataques contra os sistemas de informação e que substitui 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,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu [1],

Deliberando de acordo com o processo legislativo ordinário [2],

Considerando o seguinte:

(1) A presente diretiva tem como objetivos aproximar o direito penal dos Estados-Membros no domínio dos ataques contra os sistemas de informação, estabelecendo regras mínimas relativas à definição de infrações penais e as sanções aplicáveis, e melhorar a cooperação entre as autoridades competentes, nomeadamente a polícia e outros serviços especializados dos Estados-Membros responsáveis pela aplicação da lei, bem como as agências e organismos especializados competentes da União, tais como a Eurojust, a Europol e o seu Centro Europeu de Cibercriminalidade, e a Agência Europeia para a Segurança das Redes e da Informação (ENISA).

(2) Os sistemas de informação são um elemento essencial para a interação política, social e económica na União. A sociedade está muito e cada vez mais dependente deste tipo de sistemas. O bom funcionamento e a segurança desses sistemas na União são vitais para o desenvolvimento do mercado interno e de uma economia competitiva e inovadora. Assegurar um nível adequado de proteção dos sistemas de informação deverá ser parte integrante de um quadro eficaz e exaustivo de medidas de prevenção que acompanhe as respostas do direito penal à cibercriminalidade.

(3) Os ataques contra os sistemas de informação e, em especial, os ataques ligados à criminalidade organizada constituem uma ameaça crescente a nível da União e a nível mundial, e a eventualidade de ataques terroristas ou de natureza política contra os sistemas de informação que fazem parte da infraestrutura crítica dos Estados-Membros e da União suscita uma preocupação cada vez maior. Esta ameaça pode pôr em causa a realização de uma sociedade da informação mais segura e de um espaço de liberdade, segurança e justiça e, por conseguinte, exige uma resposta ao nível da União e cooperação e coordenação reforçadas a nível internacional.

(4) Existem na União diversas infraestruturas críticas cuja perturbação ou destruição teria um impacto transfronteiriço significativo. A necessidade de aumentar a capacidade de proteger a infraestrutura crítica da União tornou claro que as medidas contra os ciberataques deverão ser complementadas por sanções penais estritas que reflitam a gravidade desses ataques. A infraestrutura crítica pode ser entendida como um conjunto de elementos, sistemas ou partes destes situados nos Estados-Membros, essenciais para a manutenção das funções societais vitais, da saúde, da segurança e do bem-estar económico e social das pessoas, como centrais energéticas, redes de transportes ou redes governamentais, cuja perturbação ou destruição teria um impacto significativo num Estado-Membro devido à impossibilidade de continuar a assegurar tais funções.

(5) Existem provas de uma tendência para perpetrar ciberataques cada vez mais perigosos e recorrentes em larga escala contra sistemas de informação que podem frequentemente ser cruciais para os Estados-Membros ou para certas funções específicas do setor público ou privado. Esta tendência é acompanhada pelo desenvolvimento de métodos cada vez mais sofisticados, como a criação e utilização das chamadas «botnets», que implicam várias fases de um ato criminoso, cada uma das quais podendo constituir por si só um grave risco para o interesse público. A presente diretiva visa, nomeadamente, introduzir sanções penais para a criação de «botnets», a saber, o ato de estabelecer o controlo à distância de grande número de computadores mediante a respetiva contaminação com *software* maligno através de ciberataques focalizados. Uma vez criada, a rede de computadores infetados que constituem a «botnet» pode ser ativada sem o conhecimento dos utilizadores dos computadores a fim de lançar um ciberataque em grande escala, o que geralmente tem o potencial de provocar danos graves, como se refere na presente diretiva. Os Estados-Membros podem determinar o que constitui um dano grave nos termos do seu direito e da sua prática nacionais, como, por exemplo, a perturbação de serviços de sistema de importância pública significativa, ou importantes custos financeiros ou a perda de dados pessoais ou informações sensíveis.

(6) Os ciberataques em larga escala podem provocar prejuízos económicos substanciais, quer através da interrupção de sistemas de informação e comunicação, quer através da perda ou alteração de informações comerciais confidenciais importantes ou de outros dados. Deverá ser prestada especial atenção à sensibilização das pequenas e médias empresas inovadoras para as ameaças decorrentes destes ataques e para a sua vulnerabilidade aos mesmos, visto que essas empresas dependem cada vez mais do bom funcionamento e da disponibilidade de sistemas de informação, e dispõem frequentemente de recursos limitados no domínio da segurança da informação.

[1] JO C 218 de 23.7.2011, p. 130.

[2] Posição do Parlamento Europeu de 4 de julho de 2013 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 22 de julho de 2013.

(7) É importante adotar definições comuns neste domínio para assegurar uma abordagem coerente na aplicação da presente diretiva nos Estados-Membros.

(8) É necessário adotar uma abordagem comum dos elementos constitutivos das infrações penais, introduzindo como infrações comuns o acesso ilegal aos sistemas de informação, a interferência ilegal em sistemas, a interferência ilegal nos dados e a interceção ilegal.

(9) A interceção compreende, embora não necessariamente de forma exclusiva, a escuta, monitorização ou vigilância do conteúdo de comunicações e a obtenção do conteúdo de dados, quer diretamente, por meio do acesso e utilização dos sistemas de informação, quer indiretamente, através da utilização de dispositivos eletrónicos de escuta não autorizada ou de escuta por meios técnicos.

(10) Os Estados-Membros deverão prever sanções para os ataques contra os sistemas de informação. Essas sanções deverão ser efetivas, proporcionadas e dissuasivas, e deverão incluir penas de prisão e/ou sanções pecuniárias.

(11) A presente diretiva prevê sanções penais pelo menos para os casos que se revestem de alguma gravidade. Os Estados-Membros podem determinar o que constitui um caso de pouca gravidade de acordo com o seu direito e a sua prática nacionais. Pode, por exemplo, considerar-se de pouca gravidade uma infração cujos danos ou risco para os interesses públicos ou privados, como a integridade de um sistema informático ou de dados informáticos, ou a integridade, os direitos ou outros interesses de uma pessoa, sejam insignificantes ou de natureza tal que tornem desnecessária a imposição quer de sanções penais dentro dos limites legais quer de responsabilidade criminal.

(12) A identificação e comunicação das ameaças e dos riscos que representam os ciberataques e da correspondente vulnerabilidade dos sistemas de informação constituem um elemento importante para prevenir e responder com eficácia aos ciberataques e para melhorar a segurança dos sistemas de informação. A concessão de incentivos à comunicação das falhas de segurança poderá contribuir para esse efeito. Os Estados-Membros deverão procurar oferecer oportunidades para a deteção e a comunicação legais das falhas de segurança.

(13) Convém prever sanções mais severas para os casos em que os ataques contra um sistema de informação sejam perpetrados por organizações criminosas, na aceção da Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada [1], ou em que os ciberataques sejam realizados em larga escala, afetando deste modo um número significativo de sistemas de informação, nomeadamente quando visam criar uma «botnet», ou quando causam danos graves, incluindo quando são perpetrados através de uma «botnet». Deverão igualmente prever-se sanções mais severas caso os ataques sejam dirigidos contra infraestruturas críticas dos Estados-Membros ou da União.

(14) A adoção de medidas eficazes contra a usurpação de identidade e outras infrações relacionadas com a identidade constitui outro elemento importante de uma abordagem integrada contra a cibercriminalidade. A necessidade de intervenção da União contra este tipo de comportamento criminoso poderá também ser ponderada no contexto da avaliação da necessidade de um instrumento transversal e abrangente da União.

(15) Nas suas conclusões de 27 e 28 de novembro de 2008, o Conselho indicou que deveria ser desenvolvida pelos Estados-Membros e pela Comissão uma nova estratégia, tendo em conta o conteúdo da Convenção do Conselho da Europa sobre a Criminalidade Informática de 2001. Essa Convenção constitui o enquadramento legal de referência do combate à cibercriminalidade, incluindo os ataques contra os sistemas de informação. A presente diretiva baseia-se nessa Convenção. A conclusão do processo de ratificação dessa Convenção por todos os Estados-Membros o mais rapidamente possível deverá ser considerada prioritária.

(16) Tendo em conta as diferentes formas como os ataques podem ser realizados e a rápida evolução do *hardware* e do *software*, a presente diretiva faz referência a instrumentos que podem ser utilizados para cometer as infrações nela previstas. Esses instrumentos podem abranger o *software* maligno, incluindo o *software* capaz de criar «botnets», utilizado para cometer ciberataques. Mesmo que um desses instrumentos seja adequado ou especialmente adequado para cometer uma das infrações previstas na presente diretiva, pode perfeitamente ter sido produzido para um fim legítimo. Atendendo à necessidade de evitar a criminalização nos casos em que tais instrumentos sejam produzidos e colocados no mercado para fins legítimos, tais como testar a fiabilidade de produtos das tecnologias da informação ou a segurança de sistemas de informação, deverá estar preenchido, além do requisito geral de intenção, o requisito da intenção direta de utilizar esses instrumentos para cometer pelo menos uma das infrações previstas na presente diretiva.

(17) A presente diretiva não imputa responsabilidade penal nos casos em que, embora estando preenchidos os critérios objetivos que configuram as infrações nela previstas, os atos sejam cometidos sem intenção criminosa, por exemplo caso uma pessoa ignore que o acesso não era autorizado ou caso o agente esteja mandatado para testar ou proteger sistemas de informação, nomeadamente quando é incumbido por uma empresa ou por um vendedor de testar a solidez do seu sistema de segurança. No contexto da presente diretiva, as obrigações contratuais ou os acordos de restrição de acesso a sistemas de informação por via da política de utilizadores ou das condições de serviço, ou os litígios laborais relativos ao acesso aos sistemas de informação do empregador e respetiva utilização para fins privados, não deverão implicar responsabilidade penal quando o acesso nessas circunstâncias seja considerado não autorizado e constitua portanto a única base para a ação penal. A presente diretiva não prejudica o direito de acesso à informação consagrado na legislação nacional e da União, mas também não pode servir de justificação para um acesso ilegal ou arbitrário à informação.

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

(18) A prática dos ciberataques poderá ser facilitada por várias circunstâncias, por exemplo nos casos em que o autor da infração tenha acesso a sistemas de segurança inerentes aos sistemas de informação afetados no âmbito do seu emprego. No contexto do direito nacional, essas circunstâncias deverão ser devidamente tidas em conta, se for caso disso, no desenrolar dos processos penais.

(19) Os Estados-Membros deverão prever no seu direito nacional circunstâncias agravantes conformes com as regras do seu ordenamento jurídico aplicáveis na matéria. Deverão assegurar que tais circunstâncias agravantes possam ser consideradas pelos juízes ao proferirem a sentença. A apreciação dessas circunstâncias é deixada ao livre arbítrio do juiz, a par dos outros elementos factuais de cada caso.

(20) A presente diretiva não regula as condições do exercício da competência relativamente a qualquer das infrações nela referidas, como sejam a existência de um relato da vítima feito no local da prática da infração ou de uma denúncia por parte do Estado no qual a infração tenha sido cometida, ou ainda o facto de o autor da infração não ter sido sujeito a ação penal no local em que a infração foi cometida.

(21) No contexto da presente diretiva, os Estados e os organismos públicos continuam a estar plenamente obrigados a garantir o respeito dos direitos humanos e das liberdades fundamentais, em conformidade com as obrigações internacionais vigentes.

(22) A presente diretiva reforça a importância das redes, como a rede do G8 ou a rede de pontos de contacto do Conselho da Europa disponíveis 24 horas por dia e sete dias por semana. Estes pontos de contacto deverão poder prestar uma assistência efetiva, facilitando, por exemplo, a troca das informações relevantes disponíveis e a prestação de aconselhamento técnico ou de informações jurídicas para efeito de inquéritos ou procedimentos relativos a infrações penais relacionadas com sistemas de informação e dados conexos que digam respeito ao Estado-Membro requerente. Para assegurar o bom funcionamento das redes, cada ponto de contacto deverá ter a capacidade de efetuar comunicações urgentes com os pontos de contacto dos outros Estados-Membros, nomeadamente com o apoio de pessoal formado e equipado. Dada a velocidade com que os ciberataques em larga escala podem ser realizados, os Estados-Membros deverão poder responder prontamente aos pedidos urgentes provenientes desta rede de pontos de contacto. Em tais casos, pode ser oportuno que o pedido de informação seja acompanhado de um contacto telefónico, a fim de assegurar o tratamento rápido do pedido pelo Estado-Membro requerido e a transmissão de uma resposta no prazo de oito horas.

(23) A cooperação entre as autoridades públicas, por um lado, e o setor privado e a sociedade civil, por outro, é de grande importância para evitar e combater os ataques contra os sistemas de informação. É necessário promover e melhorar a cooperação entre os prestadores de serviços, os produtores, os organismos responsáveis pela aplicação da lei e as autoridades judiciais, respeitando plenamente o Estado de direito. Essa cooperação poderá incluir, por exemplo, o apoio dos prestadores de serviços na preservação de eventuais provas, no fornecimento de elementos que ajudem a identificar os autores de infrações e, em última instância, no encerramento total ou parcial, nos termos do direito e da prática nacionais, de sistemas de informação ou de funções comprometidos ou utilizados para fins ilegais. Os Estados-Membros deverão também considerar a possibilidade de criar redes de cooperação e de parceria com os prestadores de serviços e com os produtores para a troca de informações relacionadas com as infrações que recaiam no âmbito de aplicação da presente diretiva.

(24) É necessário recolher dados comparáveis sobre as infrações previstas na presente diretiva. Os dados relevantes deverão ser postos à disposição das agências e organismos especializados competentes da União, como a Europol e a ENISA, em função das respetivas atribuições e necessidades de informação, a fim de obter uma imagem mais completa do problema da cibercriminalidade e da segurança das redes e da informação a nível da União e contribuindo, desse modo, para a formulação de uma resposta mais eficaz. Os Estados-Membros deverão transmitir à Europol e ao seu Centro Europeu de Cibercriminalidade informações sobre o *modus operandi* dos infratores, para efeitos da realização de avaliações de ameaça e de análises estratégicas da cibercriminalidade, nos termos da Decisão 2009/371/JAI do Conselho, de 6 de abril de 2009, que cria o Serviço Europeu de Polícia (Europol) [1]. A prestação de informações pode facilitar uma melhor compreensão das ameaças atuais e futuras e contribuir assim para a tomada de decisões mais adequadas e focalizadas sobre o combate e a prevenção dos ataques contra os sistemas de informação.

(25) A Comissão deverá apresentar um relatório sobre a aplicação da presente diretiva e fazer as propostas legislativas necessárias, suscetíveis de conduzir a um alargamento do seu âmbito, tendo em conta a evolução no domínio da cibercriminalidade. Tal evolução pode incluir avanços tecnológicos diversos, nomeadamente os que permitam uma aplicação mais eficaz da legislação relativa a ataques contra sistemas de informação, ou que facilitem a prevenção ou minimizem o impacto de tais ataques. Para esse efeito, a Comissão deverá ter em conta as análises e os relatórios disponíveis elaborados pelos intervenientes relevantes, em particular a Europol e a ENISA.

(26) A fim de combater eficazmente a cibercriminalidade, é necessário aumentar a resiliência dos sistemas de informação, tomando as medidas adequadas para os proteger de forma mais eficaz contra os ciberataques. Os Estados-Membros deverão tomar as medidas necessárias para proteger as suas infraestruturas críticas contra os ciberataques, contexto em que deverão considerar a proteção dos seus sistemas de informação e dos dados a eles associados. A garantia de um nível adequado de proteção e segurança dos sistemas de informação pelas pessoas coletivas, por exemplo, no âmbito da prestação de serviços de comunicações eletrónicas publicamente disponíveis nos termos da legislação da União em vigor no domínio

[1] JO L 121 de 15.5.2009, p. 37.

da privacidade e da proteção das comunicações e dos dados eletrónicos, constitui uma parte essencial de uma abordagem abrangente de luta eficaz contra a cibercriminalidade. Deverão ser assegurados níveis de proteção adequados contra ameaças e vulnerabilidades razoavelmente identificáveis, de acordo com os conhecimentos técnicos e tecnológicos disponíveis em setores específicos e tendo em conta as situações concretas de cada um em matéria de tratamento de dados. Os custos e os encargos inerentes a essa proteção deverão ser proporcionais aos danos que um ciberataque poderia causar às pessoas afetadas. Os Estados-Membros são incentivados a prever, no contexto do seu direito nacional, as medidas necessárias para responsabilizar as pessoas coletivas que manifestamente não assegurem um nível adequado de proteção contra ciberataques.

(27) As consideráveis lacunas e diferenças entre as legislações e os procedimentos penais 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 judiciária efetiva nesta área. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas tenham uma dimensão transfronteiriça, o que evidencia a necessidade urgente de adotar medidas suplementares para aproximar o direito penal neste domínio. Além disso, a coordenação da ação penal contra casos de ataques a sistemas de informação deverá ser facilitada pela transposição e aplicação adequadas da Decisão-Quadro 2009/948/JAI do Conselho, de 30 de novembro de 2009, relativa à prevenção e resolução de conflitos de exercício de competência em processo penal ([1]). Os Estados-Membros deverão também, em cooperação com a União, procurar melhorar a cooperação internacional relacionada com a segurança dos sistemas de informação e das redes e dados informáticos. Deverá ser devidamente tida em conta a segurança da transferência e do armazenamento de dados em todos os acordos internacionais que impliquem o intercâmbio de dados.

(28) É essencial uma melhor cooperação entre os organismos responsáveis pela aplicação da lei e as autoridades judiciais da União para um combate eficaz contra a cibercriminalidade. Neste contexto, deverá ser incentivada a intensificação dos esforços para facultar às autoridades relevantes uma formação adequada para aumentar a compreensão da cibercriminalidade e do seu impacto e para promover a cooperação e o intercâmbio de melhores práticas, por exemplo, através das agências e organismos especializados competentes da União. Essa formação deverá ter por objetivo, nomeadamente, uma maior sensibilização para os diferentes sistemas jurídicos nacionais, os eventuais desafios jurídicos e técnicos que se colocam nas investigações criminais e a partilha de competências entre as autoridades nacionais competentes.

(29) A presente diretiva respeita os direitos humanos e as liberdades fundamentais e observa os princípios reconhecidos, nomeadamente, na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, designadamente a proteção dos dados pessoais, o respeito da vida privada, a liberdade de expressão e de informação, o direito 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. Em particular, a presente diretiva procura garantir o pleno respeito desses direitos e princípios, pelo que deve ser aplicada em conformidade.

(30) A proteção dos dados pessoais é um direito fundamental consagrado pelo artigo 16.º, n.º 1, do TFUE e pelo artigo 8.º da Carta dos Direitos Fundamentais da União Europeia. Por conseguinte, o tratamento de dados pessoais no quadro da aplicação da presente diretiva deverá ser plenamente conforme com a legislação da União aplicável à proteção de dados.

(31) Nos termos do artigo 3.º do Protocolo relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, estes Estados-Membros notificaram por escrito a sua intenção de participar na adoção e aplicação da presente diretiva.

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

(33) Atendendo a que os objetivos da presente diretiva, a saber, sujeitar os ataques contra os sistemas de informação, em todos os Estados-Membros, a sanções penais efetivas, proporcionadas e dissuasivas e melhorar e incentivar a cooperação entre autoridades judiciais e outras autoridades competentes, não podem ser suficientemente realizados pelos Estados-Membros, e podem, pois, devido à sua dimensão e efeitos, ser mais bem alcançados ao nível da União, a União pode adotar medidas em conformidade com o princípio da subsidiariedade, consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade, consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir esses objetivos.

(34) A presente diretiva visa alterar e alargar o âmbito das disposições da Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação ([2]). Dado que as alterações a introduzir são numerosas e substanciais, a Decisão-Quadro 2005/222/JAI deverá, por uma questão de clareza, ser integralmente substituída no que se refere aos Estados-Membros que participam na adoção da presente diretiva,

([1]) JO L 328 de 15.12.2009, p. 42.

([2]) JO L 69 de 16.3.2005, p. 67.

ADOTARAM A PRESENTE DIRETIVA:

Artigo 1.º

Objeto

A presente diretiva estabelece regras mínimas relativas à definição das infrações penais e das sanções no domínio dos ataques contra os sistemas de informação. Tem igualmente por objetivo facilitar a prevenção da prática desse tipo de infrações e melhorar a cooperação entre as autoridades judiciais e outras autoridades competentes.

Artigo 2.º

Definições

Para efeitos da presente diretiva, entende-se por:

a) «Sistema de informação», um dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados informáticos, bem como de dados informáticos armazenados, tratados, recuperados ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;

b) «Dados informáticos», uma representação de factos, informações ou conceitos de forma adequada para o tratamento num sistema de informação, incluindo um programa que permite que um sistema de informação execute uma dada função;

c) «Pessoa coletiva», uma entidade que beneficie do estatuto de pessoa coletiva por força do direito aplicável, excluindo Estados ou organismos públicos no exercício das suas prerrogativas de autoridade pública, e organizações internacionais de direito público;

d) «Não autorizado», um comportamento a que refere a presente diretiva, incluindo o acesso, a interferência ou a interceção, não consentido pelo proprietário ou por outro titular dos direitos do sistema ou de parte dele, ou não permitido pelo direito nacional.

Artigo 3.º

Acesso ilegal a sistemas de informação

Os Estados-Membros devem tomar as medidas necessárias para assegurar que o acesso intencional e não autorizado à totalidade ou a parte de um sistema de informação seja punível como infração penal caso a infração seja cometida mediante a violação de uma medida de segurança, pelo menos nos casos que se revistam de alguma gravidade.

Artigo 4.º

Interferência ilegal no sistema

Os Estados-Membros devem tomar as medidas necessárias para assegurar que o ato intencional e não autorizado de impedir ou interromper gravemente o funcionamento de um sistema de informação, introduzindo dados informáticos, transmitindo, danificando, apagando, deteriorando, alterando ou suprimindo esses dados, ou tornando-os inacessíveis, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.

Artigo 5.º

Interferência ilegal nos dados

Os Estados-Membros devem tomar as medidas necessárias para assegurar que o ato intencional e não autorizado de apagar, danificar, deteriorar, alterar ou suprimir dados informáticos de um sistema de informação, ou de os tornar inacessíveis, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.

Artigo 6.º

Interceção ilegal

Os Estados-Membros devem tomar as medidas necessárias para assegurar que a interceção intencional e não autorizada, através de meios técnicos, de transmissões não públicas de dados informáticos para, a partir de ou num sistema de informação, incluindo emissões eletromagnéticas de um sistema de informação que comporte esses dados, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.

Artigo 7.º

Instrumentos utilizados para cometer infrações

Os Estados-Membros devem tomar as medidas necessárias para assegurar que a produção, venda, aquisição para utilização, importação, distribuição ou qualquer outra forma de disponibilização de um dos seguintes instrumentos, não autorizadas e com o intuito da sua utilização para a prática de uma das infrações previstas nos artigos 3.º a 6.º, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade:

a) Um programa informático, concebido ou adaptado essencialmente para cometer uma das infrações previstas nos artigos 3.º a 6.º;

b) Uma senha, um código de acesso ou dados similares que permitam aceder à totalidade ou a parte de um sistema de informação.

Artigo 8.º

Instigação, cumplicidade e tentativa

1. Os Estados-Membros devem assegurar que a instigação e a cumplicidade na prática de uma infração prevista nos artigos 3.º a 7.º sejam puníveis como infrações penais.

2. Os Estados-Membros devem assegurar que a tentativa da prática de uma das infrações previstas nos artigos 4.º e 5.º seja punível como infração penal.

Artigo 9.º

Sanções

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

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 3.º a 7.º sejam puníveis com uma pena máxima de prisão não inferior a dois anos, pelo menos nos casos que se revistam de alguma gravidade.

3. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 4.º e 5.º, caso sejam cometidas intencionalmente e afetem um número significativo de sistemas de informação recorrendo a um dos

instrumentos referidos no artigo 7.º, concebido ou adaptado essencialmente para esse fim, sejam puníveis com uma pena máxima de prisão não inferior a três anos.

4. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 4.º e 5.º sejam puníveis com uma pena máxima de prisão não inferior a cinco anos caso:

a) Sejam cometidas no âmbito de uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI, independentemente da sanção nela prevista;

b) Causem danos graves; ou

c) Sejam cometidas contra um sistema de informação que constitua uma infraestrutura crítica.

5. Os Estados-Membros devem tomar as medidas necessárias para assegurar que, caso as infrações previstas nos artigos 4.º e 5.º sejam cometidas mediante a utilização abusiva de dados pessoais de outra pessoa com o objetivo de conquistar a confiança de terceiros, causando assim danos ao legítimo titular da identidade, tal possa, de acordo com o direito nacional, ser considerado uma circunstância agravante, salvo se tal circunstância já estiver abrangida por outra infração punível pelo direito nacional.

Artigo 10.º

Responsabilidade das pessoas coletivas

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as pessoas coletivas possam ser consideradas responsáveis pelas infrações previstas nos artigos 3.º a 8.º, cometidas em seu benefício por qualquer pessoa, agindo a título individual ou enquanto membro de um dos seus órgãos e que nela tenha uma posição dirigente, com base num dos seguintes elementos:

a) Poder de representação da pessoa coletiva;

b) Poderes para tomar decisões em nome da pessoa coletiva;

c) Poderes para exercer controlo dentro da pessoa coletiva.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as pessoas coletivas possam ser consideradas responsáveis caso a falta de supervisão ou de controlo por parte de uma das pessoas referidas no n.º 1 tenha tornado possível a prática, por uma pessoa sob a sua autoridade, de uma das infrações previstas nos artigos 3.º a 8.º em benefício dessa pessoa coletiva.

3. A responsabilidade das pessoas coletivas por força dos n.os 1 e 2 não exclui a ação penal contra as pessoas singulares que sejam autoras, instigadoras ou cúmplices de uma das infrações previstas nos artigos 3.º a 8.º.

Artigo 11.º

Sanções aplicáveis às pessoas coletivas

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que uma pessoa coletiva considerada responsável nos termos do artigo 10.º, n.º 1, seja passível de sanções efetivas, proporcionadas e dissuasivas, incluindo multas ou coimas e, nomeadamente:

a) A exclusão do direito a benefícios ou auxílios públicos;

b) A proibição temporária ou permanente de exercer atividades comerciais;

c) A colocação sob vigilância judicial;

d) A liquidação judicial;

e) O encerramento temporário ou definitivo dos estabelecimentos utilizados para a prática da infração.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que uma pessoa coletiva considerada responsável nos termos do artigo 10.º, n.º 2, seja passível de sanções ou de outras medidas efetivas, proporcionadas e dissuasivas.

Artigo 12.º

Competência

1. Os Estados-Membros devem determinar a sua própria competência relativamente às infrações previstas nos artigos 3.º a 8.º caso a infração tenha sido cometida:

a) Total ou parcialmente no seu território; ou

b) Por um dos seus nacionais, pelo menos nos casos em que o ato constitua infração no local em que seja praticado.

2. Ao determinarem a sua competência nos termos do n.º 1, alínea a), os Estados-Membros devem assegurar que são competentes nos casos em que:

a) O autor tenha cometido a infração quando se encontrava fisicamente presente no seu território, independentemente de a infração ter ou não sido cometida contra um sistema de informação situado nesse território; ou

b) A infração tenha sido cometida contra um sistema de informação situado no seu território, independentemente de o seu autor se encontrar ou não fisicamente presente nesse território;

3. Os Estados-Membros devem informar a Comissão caso decidam alargar a sua competência às infrações previstas nos artigos 3.º a 8.º cometidas fora do seu território, nomeadamente caso:

a) O autor tenha a sua residência habitual no seu território; ou

b) A infração tenha sido cometida em benefício de uma pessoa coletiva estabelecida no seu território.

Artigo 13.º

Troca de informações

1. Para efeitos da troca de informações relativas às infrações previstas nos artigos 3.º a 8.º, os Estados-Membros devem assegurar a existência de um ponto de contacto operacional nacional e recorrer à rede existente de pontos de contacto operacionais disponível 24 horas por dia e sete dias por semana. Os Estados-Membros devem também assegurar a existência de procedimentos que, em caso de pedidos de assistência urgentes, lhes permitam indicar, no prazo máximo de oito horas a contar da receção do pedido, se o pedido de ajuda será deferido, e a forma e o prazo estimado de resposta.

2. Os Estados-Membros devem informar a Comissão do seu ponto de contacto referido no n.º 1. A Comissão deve transmitir essa informação aos restantes Estados-Membros e às agências e órgãos especializados competentes da União.

3. Os Estados-Membros devem tomar as medidas necessárias para assegurar a disponibilização de canais de comunicação adequados para facilitar a comunicação sem atrasos indevidos das infrações previstas nos artigos 3.º a 6.º às autoridades nacionais competentes.

Artigo 14.º

Acompanhamento e estatísticas

1. Os Estados-Membros devem assegurar a criação de um sistema de registo, produção e disponibilização de dados estatísticos sobre as infrações previstas nos artigos 3.º a 7.º.

2. As estatísticas referidas no n.º 1 devem abranger, no mínimo, os dados existentes sobre o número de infrações previstas nos artigos 3.º a 7.º registadas pelos Estados-Membros, e sobre o número de pessoas alvo de ação penal e condenadas pelas infrações previstas nos artigos 3.º a 7.º.

3. Os Estados-Membros devem transmitir à Comissão os dados recolhidos nos termos do presente artigo. A Comissão deve assegurar a publicação de uma revisão consolidada destes relatórios estatísticos e a sua transmissão às agências e organismos especializados competentes da União.

Artigo 15.º

Substituição da Decisão-Quadro 2005/222/JAI

A Decisão-Quadro 2005/222/JAI é substituída, no que diz respeito aos Estados-Membros que participam na adoção da presente diretiva, sem prejuízo das obrigações dos Estados-Membros quanto ao prazo de transposição daquela decisão-quadro para o direito nacional.

No que diz respeito aos Estados-Membros que participam na adoção da presente diretiva, as remissões para a Decisão-Quadro 2005/222/JAI devem entender-se como sendo feitas para a presente diretiva.

Artigo 16.º

Transposição

1. Os Estados-Membros põem em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva até 4 de setembro de 2015.

2. Os Estados-Membros comunicam à Comissão o texto das disposições que transpõem para o respetivo direito interno as obrigações que sobre eles impendem por força da presente diretiva.

3. Quando os Estados-Membros adotarem essas disposições, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência aquando da sua publicação oficial. As modalidades dessa referência são estabelecidas pelos Estados-Membros.

Artigo 17.º

Relatórios

Até 4 de setembro de 2017, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório no qual avalie em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à presente diretiva, acompanhado, se necessário, de propostas legislativas. A Comissão deve também ter em conta o progresso técnico e jurídico em matéria de cibercriminalidade, particularmente no que respeita ao âmbito de aplicação da presente diretiva.

Artigo 18.º

Entrada em vigor

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

Artigo 19.º

Destinatários

Os destinatários da presente diretiva são os Estados-Membros, nos termos dos Tratados.

Feito em Bruxelas, em 12 de agosto de 2013.

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*
M. SCHULZ	L. LINKEVIČIUS