PROPOSTA DE LEI N.º 289/X/4ª

Exposição de Motivos

A expansão das redes de comunicação tornou a *Internet* uma realidade omnipresente. Todas as actividades das sociedades modernas e das economias usam a Internet para seu apoio. Os cidadãos socorrem-se da Internet na sua vida quotidiana e os Estados apoiam nela as suas tradicionais funções. Neste contexto, foi natural o surgimento de actividades ilegais associadas às redes de comunicação, usando-as e explorando as suas vulnerabilidades, criando assim riscos para a utilização quotidiana dos meios informáticos. A cibercriminalidade tornou-se, portanto, uma ameaça dos tempos modernos.

Os Estados têm vindo a adoptar medidas visando prevenir e contrariar as práticas ilegais e abusivas nas redes de comunicação. Portugal tem, desde 1991, por impulso da recomendação R (89) 9 do Conselho da Europa, um quadro normativo que visa punir aquilo a que chamou os crimes informáticos: a Lei n.º 109/91, de 17 de Agosto. Este diploma, adequado à realidade que se destinava a regular na data em que entrou em vigor, pelo decurso de quase duas décadas, tornou-se deficitário.

Nas redes de informação e comunicação surgiram entretanto novas realidades que têm vindo a ser descritas e consideradas como crime por muitas outras legislações europeias e por instrumentos internacionais. É, por exemplo, o caso da produção ou difusão de vírus e outros programas maliciosos, realidades ainda não consagradas na lei nacional: de facto, no actual quadro normativo, quem produzir e/ou difundir vírus e outros dispositivos desta natureza não incorrerá, por esses factos, na prática de nenhum crime, nem será punido por essa actuação. Não obstante, é sobejamente conhecida a nocividade que resulta da produção e difusão de vírus informáticos pelas redes de comunicações. Essa é a razão pela qual muitas outras legislações optaram pela criminalização desta actividade, na sequência, aliás, da disposição do artigo 6.º da Convenção sobre Cibercrime do Conselho da Europa.

A Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra sistemas de informação, descreve comportamentos que deverão ser qualificados como crime, obrigando também à criação de normas conexas, relacionadas com tais comportamentos, atinentes à instigação, auxílio, cumplicidade e tentativa, responsabilidade de pessoas colectivas, competência territorial e ainda intercâmbio de informações. A transposição da Decisão-Quadro supõe, para o ordenamento jurídico

português, a alteração ao regime da criminalidade informática, hoje previsto na chamada Lei da Criminalidade Informática (a já referida Lei n.º 109/91, de 17 de Agosto).

A 23 de Novembro de 2001, Portugal assinou a Convenção sobre Cibercrime do Conselho da Europa, cujo processo de ratificação se encontra agora em curso. A Convenção é o primeiro e mais importante trabalho internacional de fundo sobre crime no ciberespaço. Tem vocação universal e pretende-se que venha a ser aceite pela generalidade dos países do Mundo. Pretende harmonizar as várias legislações nacionais sobre a matéria, propiciar e facilitar a cooperação internacional e facilitar as investigações de natureza criminal. Incide sobre direito penal material (definindo crimes contra a confidencialidade, integridade e disponibilidade dos sistemas de computadores, crimes referentes aos conteúdos e crimes cometidos por via da informática), mas inclui também medidas processuais e de cooperação judiciária internacional. O acolhimento das obrigações legislativas decorrentes da Convenção imporá também a alteração do regime actualmente vigente.

A adequação ao quadro jurídico da Convenção trará consigo, designadamente, uma vantagem especial de adesão a um espaço europeu de cooperação, com projecção policial e judiciária. Em concreto, trará também a possibilidade de, em processos a decorrer, utilizar novas formas de investigação e novas vias de cooperação, quando se tornar necessário recorrer à cooperação internacional. Estas novas formas de investigar e de cooperar podem utilizar-se quanto a crimes previstos na Convenção, mas também para investigar outros crimes, desde que cometidos por via de sistemas de computadores e ainda para qualquer tipo de crimes, desde que haja prova dos mesmos sob forma electrónica.

Na generalidade, em termos estruturais, no que respeita ao direito penal material, pode afirmar-se que a transposição da Decisão-Quadro n.º 2005/222/JAI e a consagração das obrigações legais resultantes da Convenção supõem apenas ajustamentos da actual legislação sobre criminalidade informática. Ressalvam-se as novas formas de criminalidade, algumas das quais já referidas e em relação às quais a legislação portuguesa tem sido considerada deficitária.

Já no campo das normas de direito processual penal, a desadequação da ordem jurídica nacional às novas realidades a implementar é superior. A recente revisão do Código de Processo Penal optou pela limitação, em abstracto, da possibilidade de realização de intercepções de comunicações telefónicas e electrónicas, não tendo incluído normas especiais para a área da cibercriminalidade. Assim, não está prevista a obtenção de dados de

tráfego nem a realização de intercepção de comunicações electrónicas na investigação de crimes não previstos no artigo 187.º do Código de Processo Penal. Entre eles, encontram-se crimes previstos na Lei n.º 109/91, de 17 de Agosto, bem como crimes contra a propriedade intelectual cometidos por via de redes informáticas. A realização de intercepções de comunicações electrónicas e, sobretudo, a obtenção de dados de tráfego, são ferramentas processuais essenciais em processo-crime em que se investiguem crimes cometidos por via das redes de comunicações, tendo essa preocupação ficado espelhada no diploma que obriga os operadores de comunicações a guardarem os dados de tráfego dos seus clientes, tendo em vista a sua eventual necessidade em investigação criminal – Lei n.º 32/2008, de 17 de Julho, que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas. Importa assim superar o actual regime, de modo a fornecer ao sistema processual penal normas que permitam a obtenção de dados de tráfego e a realização de intercepções de comunicações em investigações de crimes praticados no ambiente virtual. É o que se pretende fazer por via da lei que agora se propõe.

Optou-se por condensar neste diploma todas as normas respeitantes à cibercriminalidade e não por proceder à alteração das várias fontes legislativas sobre a matéria – além da própria Lei da Criminalidade Informática, o Código Penal, o Código de Processo Penal e a Lei da Cooperação Judiciária Internacional (Lei n.º 144/99, de 31 de Agosto, com as suas alterações). Afigura-se ser esta a opção legislativa mais coerente com a tradição portuguesa, onde existem, especificamente na área penal, outros diplomas estruturantes de matérias na especialidade: assim acontece com a criminalidade relacionada com estupefacientes, com os crimes contra a economia ou com a criminalidade fiscal, cujos quadros penais e processuais penais específicos estão definidos em diploma próprio. No que respeita às regras processuais, militando a favor desta solução, existem ainda duas outras razões: por um lado, a geral inconveniência de ver em diplomas estruturantes do ordenamento penal regras especiais, apenas aplicáveis a uma parcela muito restrita dos tipos de ilícito; por outro, a conveniência prática, para os operadores judiciários, de ver sistematizados todos os normativos referentes a um sector específico da criminalidade.

Em suma, quanto ao direito penal material, em cumprimento das obrigações assumidas no âmbito da Decisão-Quadro e da Convenção, introduzem-se agora alterações legislativas de ajustamento do actual regime.

Assim é quanto às definições, incluídas no artigo 2.º, no qual se introduz o conceito de «dados informáticos», em substituição do conceito mais limitado e hoje em dia insuficiente de «programa informático». Acrescentam-se as definições, modernas e não existentes em 1991, de «fornecedor de serviço» e de «dados de tráfego». É alterado o conceito de «sistema informático», que passa a ser mais abrangente, incluindo-se nele, por exemplo, dispositivos como os telemóveis. Suprime-se, por deixar de fazer sentido face a este último, o conceito de «rede informática».

Quanto à responsabilidade de pessoas colectivas e a várias outras regras de punição de pessoas singulares e colectivas, optou-se pela revogação do regime específico criado em 1991 a este propósito. Em seu lugar, remete-se para o regime geral de responsabilização de pessoas colectivas, previsto no Código Penal. Desta forma satisfazem-se os compromissos assumidos pela Decisão-Quadro e pela Convenção, da mesma forma que se simplifica o quadro normativo, eliminando um regime especial de responsabilização, criada em 1991 pela inexistência de um regime geral, mas agora já não justificado, após a introdução desse mesmo regime geral na alteração do Código Penal operada em 2007.

Quanto aos tipos de crime de dano informático, sabotagem informática, acesso ilegítimo e intercepção ilegítima, foram feitos ajustamentos na redacção, tendo em vista, por um lado, actualizar o texto legal e, por outro, consagrar novas modalidades de acção típica.

A propósito da competência jurisdicional, a Convenção prevê uma inovação face ao que já resulta dos artigos 4.º e 5.º do Código Penal, traduzida na obrigação de os Estados signatários se declararem competentes para prosseguirem criminalmente, independentemente do local da prática dos factos, os seus cidadãos nacionais, se a infracção for punível no local onde foi cometida ou não for da competência de nenhum Estado. Apesar de esta solução não estar anteriormente consagrada na lei portuguesa, já se prevê, para certos crimes a competência universal da lei portuguesa.

No âmbito das disposições processuais, foram introduzidas a preservação expedita de dados armazenados num computador e a preservação expedita e revelação de dados de tráfego, em cumprimento das obrigações resultantes dos artigos 16.º e 17.º da Convenção. Foi introduzido o mecanismo da injunção (cfr. artigo 18.º da Convenção) e adaptados os regimes das buscas e das apreensões, já largamente previstas na legislação processual penal,

às investigações de crimes cometidos no ambiente virtual. Na verdade, a essência destas medidas processuais coincide, no ambiente do ciberespaço, com as clássicas formas de busca e apreensão, do processo penal. Porém, a forma como a busca e a apreensão estão descritas no Código de Processo Penal exigiam alguma adequação a estas novas realidades.

Do mesmo modo, foi adaptado para este diploma o regime de intercepção de comunicações, previsto no Código de Processo Penal para as comunicações telefónicas. Na verdade, o Código prevê já uma extensão do regime das intercepções telefónicas a outras comunicações, por exemplo electrónicas. Todavia, essa extensão não resolve o problema da investigação de crimes informáticos ou relacionados com a informática, porque o âmbito de aplicação deste regime, por via da extensão, é o mesmo das intercepções telefónicas. Ora, torna-se necessário abranger os crimes informáticos em geral, bem como aqueles cometidos por via de computadores, assim se motivando a criação de norma especial. Esta norma adopta em geral as regras do Código de Processo Penal, que é adaptado em função da especificidade dos crimes a que, por via desta nova lei, é aplicável.

A adopção, para a investigação de crimes informáticos, de medidas processuais especiais, significa necessariamente uma compressão das liberdades dos cidadãos no ciberespaço. É óbvia para todos a enorme vantagem da existência de um espaço livre e praticamente desregulado, onde cada um pode livremente comunicar, informar-se e informar, bem como – e talvez acima de tudo –, expressar-se e manifestar-se sem censura nem constrangimentos. A verdade, porém, é que ninguém é alheio às emergentes realidades criminosas, de sinal oposto, que beneficiam da capacidade de comunicação massiva, eficaz e de custo reduzidíssimo, escolhendo as suas vítimas de forma quase indiscriminada, por todo o Mundo, resguardando-se das autoridades por detrás da fronteira, do anonimato e da complexidade técnica. Se é verdade que a *Internet* não é propriedade de ninguém, também o é que ninguém é directamente responsável por ela nem pelo que nela ocorre. Não tem sede, nem local, onde se possam localizar os seus responsáveis. As leis modernas têm que tratar de forma adequada as novas realidades criminógenas, incriminando-as e dotando as entidades competentes das ferramentas necessárias à sua investigação e julgamento.

Refira-se, finalmente, que na área da cooperação internacional se remete, como regra, para regimes legais já em vigor. Além disso, assume-se que as autoridades portuguesas podem

solicitar cooperação internacional – e também receber e executar pedidos de cooperação provenientes de autoridades estrangeiras –, nas mesmas condições e circunstâncias em que actuariam se os factos criminosos estivessem a ser investigados em Portugal. Cria-se um ponto permanente de contacto 24 horas/7dias, no seio da Polícia Judiciária, ao qual compete assegurar, quanto à matéria a que respeita esta proposta de lei, um papel essencial na cooperação internacional emergente.

Foram ouvidos a Procuradoria-Geral da República, o Conselho Superior de Magistratura e a Comissão Nacional de Protecção de Dados.

Foi promovida a audição da Ordem dos Advogados.

Deve ser desencadeada a audição do Conselho Superior do Ministério Público.

Assim:

Nos termos da alínea *d)* do n.º 1 do artigo 197.º da Constituição, o Governo apresenta à Assembleia da República a seguinte proposta de lei:

CAPÍTULO I

Objecto e definições

Artigo 1.º

Objecto

A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Artigo 2.º

Definições

Para efeitos da presente lei, considera-se:

a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em

execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;

b) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;

c) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;

d) «Fornecedor de serviço», qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores;

e) «Intercepção», o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;

f) «Topografia», uma série de imagens entre si ligadas, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho ou parte dele de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;

g) «Produto semicondutor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.

CAPÍTULO II

Disposições penais materiais

Artigo 3.º

Falsidade informática

1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até cinco anos ou multa de 120 a 600 dias.

2 - Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de um a cinco anos de prisão.

3 - Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.

4 - Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de um a cinco anos.

5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de dois a cinco anos.

Artigo 4.º

Dano relativo a programas ou outros dados informáticos

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou

em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até três anos ou pena de multa.

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3 - Se o dano causado for de valor elevado, a pena é a de prisão até cinco anos ou de multa até 600 dias.

4 - Se o dano causado for de valor consideravelmente elevado, a pena é a de prisão de um a 10 anos.

5 - Com excepção dos casos previstos no n.º 2, a tentativa é punível.

6 - Nos casos previstos nos n.ºs 1, 3 e 5 o procedimento penal depende da queixa.

Artigo 5.º

Sabotagem informática

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até cinco anos ou com pena de multa até 600 dias.

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3 - A pena é a de prisão de um a cinco anos se o dano emergente da perturbação for de valor elevado.

4 - A pena é a de prisão de um a 10 anos se:

a) O dano emergente da perturbação for de valor consideravelmente elevado;

b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

5 - Com excepção dos casos previstos n.º 2, a tentativa é punível.

Artigo 6.º

Acesso ilegítimo

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até um ano ou com pena de multa até 120 dias.

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3 - A pena é a de prisão até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.

4 - A pena é a de prisão de um a cinco anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

5 - Com excepção dos casos previstos no n.º 2, a tentativa é punível.

6 - Nos casos previstos nos n.º s 1, 3 e 5 o procedimento penal depende de queixa.

Artigo 7.º

Intercepção ilegítima

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele proveniente, é punido com pena de prisão até três anos ou com pena de multa.

2 - A tentativa é punível.

3 - Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.

Artigo 8.º

Reprodução ilegítima de programa protegido

1 - Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até três anos ou com pena de multa.

2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

3 - A tentativa é punível.

Artigo 9.º

Associação criminosa

1 - Quem promover ou fundar grupo, organização ou associação cuja finalidade ou actividade seja dirigida à prática de um ou mais dos crimes aos quais a presente lei é aplicável, é punido com pena de prisão de um a cinco anos.

2 - Na mesma pena incorre quem fizer parte de tais grupos, organizações ou associações ou quem os apoiar, nomeadamente fornecendo armas, munições, instrumentos de crime, guarda ou locais para as reuniões, ou qualquer auxílio para que se recrutem novos elementos.

3 - Quem chefiar ou dirigir os grupos, organizações ou associações referidos nos números anteriores é punido com pena de prisão de dois a oito anos.

4 - As penas referidas podem ser especialmente atenuadas ou não ter lugar a punição se o agente impedir ou se esforçar seriamente por impedir a continuação dos grupos, organizações ou associações, ou comunicar à autoridade a sua existência de modo a esta poder evitar a prática de crimes.

5 - Para os efeitos do presente artigo, considera-se que existe grupo, organização ou associação quando esteja em causa um conjunto de, pelo menos, três pessoas actuando concertadamente durante um certo período de tempo.

Artigo 10.º

Responsabilidade penal das pessoas colectivas e entidades equiparadas

As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal.

Artigo 11.º

Perda de bens

1 - Sem prejuízo do disposto no Código Penal em matéria de perda de instrumentos, produtos e vantagens relacionados com um crime, são sempre declarados perdidos a favor do Estado os objectos, materiais, equipamentos ou dispositivos que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem a pessoa que tenha sido condenada pela sua prática.

2 - À avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal que sejam susceptíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto no Decreto-Lei n.º 11/2007, de 19 de Janeiro.

CAPÍTULO III

Disposições processuais

Artigo 12.º

Âmbito de aplicação das disposições processuais

1 - O disposto no presente capítulo aplica-se a processos relativos a crimes:

a) Previstos na presente lei; ou

b) Cometidos por meio de um sistema informático.

2 - O disposto no presente capítulo aplica-se ainda a processos relativos a crimes em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, com excepção dos artigos 13.º e 20.º, que apenas se aplicam a tais crimes na medida em que os mesmos se encontrem previstos no artigo 187.º do Código de Processo Penal.

Artigo 13.º

Transmissão de dados de tráfego e de localização e dados conexos

A transmissão de dados conservados ao abrigo da Lei n.º 32/2008, de 17 de Julho, pode ser ordenada nos termos, condições e circunstâncias previstos nesse diploma.

Artigo 14.º

Preservação expedita de dados

1 - Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.

2 - A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

3 - A ordem de preservação discrimina, sob pena de nulidade:

a) A natureza dos dados;

b) A sua origem e destino, se forem conhecidos; e

c) O período de tempo pelo qual deverão ser preservados, até um máximo de três

meses.

4 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção.

5 - A autoridade judiciária competente, ou o órgão de polícia criminal mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c)* do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

6 - Tratando-se de ordem de preservação expedita de dados conservados ao abrigo da Lei n.º 32/2008, de 17 de Julho, aplica-se-lhe o disposto nesse diploma.

Artigo 15.º

Revelação expedita de dados de tráfego

Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

Artigo 16.º

Injunção para apresentação ou concessão do acesso a dados

1 - Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

2 - A ordem referida no número anterior identifica tanto quanto possível os dados em causa.

3 - Em cumprimento da ordem descrita nos n.ºs 1 e 2, quem tenha disponibilidade ou

controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.

4 - O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:

a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou

c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

5 - A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo.

6 - Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária.

Artigo 17.º

Pesquisa de dados informáticos

1 - Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias,

sob pena de nulidade.

3 - O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:

a) No caso previsto na alínea *b*), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;

b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.

5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.ºs 1 e 2.

6 - À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal.

Artigo 18.º

Apreensão de dados informáticos

1 - Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

2 - O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e

executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

3 - Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

4 - As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

5 - As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal.

6 - A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente revestir as formas seguintes:

a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;

b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou

d) Eliminação não reversível ou bloqueio do acesso aos dados.

7 - No caso da apreensão efectuada nos termos da alínea *b)* do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.

Artigo 19.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que

seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 20.º

Intercepção de comunicações

1 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.

2 - A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.

3 - No demais, é aplicável à intercepção e registo de transmissões de dados informáticos o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.

Artigo 21.º

Acções encobertas

1 - É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:

a) Os previstos na presente lei;

b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a cinco anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, os crimes previstos nos artigos 218.º, 221.º e 240.º do Código Penal, bem como os crimes consagrados no Título IV do Código do Direito de Autor e dos Direitos Conexos.

2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.

CAPÍTULO IV

Cooperação internacional

Artigo 22.º

Âmbito da cooperação internacional

As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime.

Artigo 23.º

Ponto de contacto permanente para a cooperação internacional

1 - Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, 24 horas por dia, sete dias por semana.

2 - Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Portugal se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais.

3 - A assistência imediata prestada por este ponto de contacto permanente inclui:

a) A prestação de aconselhamento técnico a outros pontos de contacto;

b) A preservação expedita de dados nos casos de urgência ou perigo na demora, em conformidade com o disposto no artigo seguinte;

c) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora;

d) A localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora;

e) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas *b*) a *d*), fora dos casos aí previstos, tendo em vista a sua rápida execução.

4 - Sempre que actue ao abrigo das alíneas *b*) a *d*) do número anterior, a Polícia Judiciária

dá notícia imediata do facto ao Ministério Público e remete-lhe o relatório previsto nos termos do artigo 253.º do Código de Processo Penal.

Artigo 24.º

Preservação e revelação expeditas de dados informáticos em cooperação internacional

1 - Pode ser solicitada a Portugal a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 12.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

2 - A solicitação específica:

a) A autoridade que pede a preservação;

b) A infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados;

c) Os dados informáticos a conservar e a sua relação com a infracção;

d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático;

e) A necessidade da medida de preservação; e

f) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados.

3 - Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve.

4 - A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior.

5 - A ordem de preservação específica, sob pena de nulidade:

a) A natureza dos dados;

b) Se forem conhecidos, a origem e o destino dos mesmos; e

c) O período de tempo pelo qual os dados devem ser preservados, até um máximo

de três meses.

6 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade.

7 - A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do n.º 5, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

8 - Quando seja apresentado o pedido de auxílio referido no n.º 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido.

9 - Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos:

a) À autoridade judiciária competente, em execução do pedido de auxílio referido no n.º 1, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo dos artigos 15.º a 19.º;

b) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo do artigo 15.º

10 - A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efectuada, comunica-os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos.

11 - O disposto nos n.ºs 1 e 2 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades portuguesas.

Artigo 25.º

Motivos de recusa

1 - A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando:

a) Os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do Direito português;

b) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos.

2 - A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.

Artigo 26.º

Acesso a dados informáticos em cooperação internacional

1 - Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal, relativos a crimes previstos no artigo 12.º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante.

2 - A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em instrumento internacional aplicável.

3 - O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

Artigo 27.º

Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, podem:

a) Aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis;

b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los.

Artigo 28.º

Intercepção de comunicações em cooperação internacional

1 - Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 20.º, em caso nacional semelhante.

2 - É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa para autorização.

3 - O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido.

4 - O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

CAPÍTULO V

Disposições finais e transitórias

Artigo 29.º

Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses

1 - Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal portuguesa é ainda aplicável a factos:

a) Praticados por portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;

b) Cometidos em benefício de pessoas colectivas com sede em território português;

c) Fisicamente praticados em território português, ainda que visem sistemas

informáticos localizados fora desse território; ou

d) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.

2 - Se, em função da aplicabilidade da lei penal portuguesa, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei os tribunais portugueses e os tribunais de outro Estado membro da União Europeia, podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente recorre aos órgãos e mecanismos instituídos no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados-membros e a coordenação das respectivas acções, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infracção, tendo em vista centralizá-lo num só deles.

3 - A decisão de aceitação ou transmissão do procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos:

a) O local onde foi praticada a infracção;

b) A nacionalidade do autor dos factos; e

c) O local onde o autor dos factos foi encontrado.

4 - São aplicáveis aos crimes previstos na presente lei as regras gerais de competência dos tribunais previstas no Código de Processo Penal.

5 - Em caso de dúvida quanto ao tribunal territorialmente competente, designadamente por não coincidirem o local onde fisicamente o agente actuou e o local onde está fisicamente instalado o sistema informático visado com a sua actuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos.

Artigo 30.º

Regime geral aplicável

Em tudo o que não contrarie o disposto na presente lei, aplicam-se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respectivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei n.º 144/99, de 31 de Agosto.

Artigo 31.º

Competência da Polícia Judiciária para a cooperação internacional

A competência atribuída pela presente lei à Polícia Judiciária para efeitos de cooperação internacional é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei.

Artigo 32.º

Protecção de dados pessoais

O tratamento de dados pessoais ao abrigo da presente lei efectua-se de acordo com o disposto na Lei n.º 67/98, de 26 de Outubro, sendo aplicável, com as necessárias adaptações, o disposto no capítulo VI desse diploma.

Artigo 33.º

Norma revogatória

É revogada a Lei n.º 109/91, de 17 de Agosto.

Artigo 34.º

Entrada em vigor

A presente lei entra em vigor 30 dias após a sua publicação.

Visto e aprovado em Conselho de Ministros de 14 de Maio de 2009

O Primeiro-Ministro

O Ministro da Presidência

O Ministro dos Assuntos Parlamentares