os bens ou direitos objeto da garantia e respetivos dados de identificação registral, se aplicável;

A existência de eventuais garantias pessoais, com identificação dos garantes;

A taxa de juros moratórios aplicável.

É designado o dia 05-07-2012, pelas 14:00 horas, por despacho proferido em 17-05-2012, para a realização da reunião de assembleia de credores de apreciação do relatório, tendo ficado a data anteriormente designada ficado sem efeito, podendo fazer-se representar por mandatário com poderes especiais para o efeito.

É facultada a participação de até três elementos da Comissão de Trabalhadores ou, na falta desta, de até três representantes dos trabalhadores por estes designados (n.º 6 do Artigo 72.º do CIRE).

Da presente sentença pode ser interposto recurso, no prazo de 15 dias (artigo 42.º do CIRE), e ou deduzidos embargos, no prazo de 5 dias (artigo 40.º e 42 do CIRE).

Com a petição de embargos, devem ser oferecidos todos os meios de prova de que o embargante disponha, ficando obrigado a apresentar as testemunhas arroladas, cujo número não pode exceder os limites previstos no artigo 789.º do Código de Processo Civil (alínea c do n.º 2 do artigo 24.º do CIRE).

Ficam ainda advertidos que os prazos para recurso, embargos e reclamação de créditos só começam a correr finda a dilação e que esta se conta da publicação do anúncio.

Os prazos são contínuos, não se suspendendo durante as férias judiciais (n.º 1 do artigo 9.º do CIRE).

Terminando o prazo em dia que os tribunais estiverem encerrados, transfere-se o seu termo para o primeiro dia útil seguinte.

Informação — Plano de Insolvência

Pode ser aprovado Plano de Insolvência, com vista ao pagamento dos créditos sobre a insolvência, a liquidação da massa e a sua repartição pelos titulares daqueles créditos e pelo devedor (artigo 192.º do CIRE).

Podem apresentar proposta de Plano de Insolvência o administrador da insolvência, o devedor, qualquer pessoa responsável pelas dívidas da insolvência ou qualquer credor ou grupo de credores que representem um quinto do total dos créditos não subordinados reconhecidos na sentença de graduação de créditos ou, na falta desta, na estimativa do Sr. Juiz (artigo 193.º do CIRE).

17-05-2012. — A Juíza de Direito, *Dr.ª Alexandra Ferreira.* — O Oficial de Justiça, *Dulce Maria Mota Ramos*.

306117747

MINISTÉRIO PÚBLICO

Procuradoria-Geral da República

Parecer n.º 11/2011

Software — Programa do computador — Crime informático — Cibercrime — Pirataria informática — Reprodução ilegítima — Órgãos de polícia criminal — Investigação criminal — Pesquisa de dados informáticos — Preservação expedita de dados — Apreensão — competência — Competência reservada — Polícia judiciária — Autoridade de segurança alimentar e económica — Atividade económica — Fiscalização — Direitos de autor — Propriedade intelectual.

1.ª O crime de reprodução ilegítima de programa protegido, previsto e punido pelo artigo 8.º da lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, assume a natureza de crime informático, como tal legalmente tipificado, e a sua prática envolve a utilização de um sistema informático, pelo que lhe são aplicáveis as disposições processuais contidas nos artigos 12.º a 17.º daquele diploma, conforme dispõe o seu artigo 11.º, n.º 1, alíneas *a*) e *b*), da mesma lei;

2.ª A competência para a investigação do crime de reprodução ilegítima de programa protegido, enquanto crime informático, está reservada à Polícia Judiciária, em conformidade com o disposto no artigo 7.º, n.º 3, alínea *l*), da Lei de Organização da Investigação Criminal, aprovada pela Lei n.º 49/2008, de 27 de agosto, podendo somente em tal entidade ser delegada a execução de atos de inquérito pelo Ministério Público;

3.ª A atuação da Autoridade de Segurança Alimentar e Económica (ASAE) no âmbito do crime referido na conclusão anterior, está limitada exclusivamente à prática dos atos cautelares e urgentes, quer para obstar à sua consumação, quer para assegurar os respetivos meios de prova;

4.ª No decurso das suas ações de fiscalização de atividades económicas, a ASAE deve, nos termos do disposto no artigo 201.º, n.º 2, do Código do Direito de Autor e dos Direitos Conexos, aprovado pelo Decreto-Lei n.º 63/85, de 14 de março, e nos artigos 178.º, n.º 4, e 249.º, n.ºs 1 e 2, alínea *c*), do Código de Processo Penal, proceder à apreensão dos suportes físicos exteriores de computador que contenham programas informáticos objeto de contrafação, bem como dos próprios computadores ou outros equipamentos informáticos em relação aos quais existam fundadas suspeitas de terem instalados programas não licenciados, comunicando o facto à Polícia Judiciária, em prazo não excedente a 24 horas, e ao Ministério Público para sua validação;

5.ª Por força da competência reservada da Polícia Judiciária para a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, nos quais se compreende o crime de reprodução não autorizada de programa protegido, está vedada à ASAE a pesquisa de dados informáticos armazenados em sistemas informáticos.

Senhor Procurador-Geral da República,

Excelência:

I

A Autoridade de Segurança Alimentar e Económica (ASAE) solicitou a Vossa Excelência a emissão de «parecer sobre a questão das competências da ASAE no domínio da Lei n.º 109/2009, de 15 de setembro, uma vez que este organismo tem-se deparado com entendimentos diferentes por parte da magistratura do Ministério Público».

No pedido ([1]), a questão é apresentada e enquadrada juridicamente nos seguintes termos:

«[...] a Lei n.º 109/2009, de 15 de setembro, que estabelece as disposições penais materiais e processuais no domínio do cibercrime e da recolha de prova em suporte eletrónico, veio revogar a Lei n.º 109/91, de 17 de agosto, estabelecendo disposições processuais especiais relativas aos crimes nela previstos, designadamente, instituindo a necessidade de autorização ou despacho da autoridade judiciária competente, para a preservação ou pesquisa de dados informáticos específicos armazenados num sistema informático, bem como para apreensão de dados informáticos, correio eletrónico ou registos informáticos de natureza semelhante.

Dos crimes previstos na Lei n.º 109/2009, de 15 de setembro, o crime usualmente investigado pela ASAE consta no seu *artigo 8.º, sob a epígrafe* "Reprodução ilegítima de programa protegido", cuja redação é praticamente idêntica à que constava na anterior Lei n.º 109/91, de 17 de agosto.

Esta disposição legal está expressamente vocacionada para o problema da "pirataria" informática e constitui a estrutura base de proteção penal dos direitos de propriedade intelectual sobre os programas.

O bem jurídico protegido é aqui a propriedade ou direitos de autor (Decreto-Lei n.º 252/94, de 20.10).

Assim, o conceito de reprodução ilegítima implicará a interpretação por referência ao ato de reprodução ser destinado a explorar economicamente uma obra à revelia do autor.

Este tipo de crime não se confunde com o comummente designado *crime informático*, que se refere a toda a atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime.

Ora, dada a natureza do crime de reprodução ilegítima de programa protegido, para a investigação do mesmo, não se nos afigura que seja necessário preservar ou pesquisar dados informáticos, correio eletrónico ou registos informáticos de natureza semelhante.

De facto, apenas se procura pesquisar os programas instalados e que não possuam a necessária licença.

Para tal, afigura-se-nos *não ser necessário obter a autorização da autoridade judiciária competente*, não sendo aqui aplicáveis as normas constantes dos artigos 12.º, 15.º, 16.º e 17.º da nova Lei n.º 109/2009, de 15 de setembro.

Por fim, importa ainda abordar a questão da competência da ASAE para investigar o crime previsto no citado artigo 8.º da Lei n.º 109/2009, de 15 de setembro, face ao disposto no artigo 7.º da Lei n.º 49/2008, de 27 de agosto, que aprova a Lei de Organização da Investigação Criminal (LOIC).

Nos termos da alínea *l*) do n.º 3 do artigo 7.º da LOIC, é da competência reservada da Polícia Judiciária a investigação dos crimes informáticos e praticados com recurso a tecnologia informática.

Ora, tal como já atrás implícito, somos de parecer que o crime de "Reprodução ilegítima de programa protegido", embora inserido numa lei designada por lei do Cibercrime, não é verdadeiramente um crime informático, uma vez que está em causa uma atividade onde

um computador, ou uma rede de computadores, é utilizada como uma ferramenta, uma base de ataque ou como um meio de crime.

O crime informático é o crime contra o computador (atividade que irá causar algum tipo de dano à máquina da vítima) ou o crime através do computador (utilizar-se de um computador para obter dados sobre o usuário da máquina).

Desta forma, em nosso entender, torna-se essencial apurar, com rigor, em que moldes a ASAE deve atuar no âmbito da Lei n.º 109/2009, de 15 de setembro.»

Em comunicação posterior ([2]), a mesma entidade mantém o entendimento de que a natureza do crime de reprodução ilegítima de programa protegido (artigo 8.º da Lei n.º 109/2009, de 15 de setembro) «não é, verdadeiramente, a de um crime informático», com a possibilidade de «se prescindir da obtenção de prévia autorização por parte da autoridade judiciária competente, o que permitirá uma maior agilização e operacionalidade no combate a este ilícito».

Cumpre emitir parecer.

II

O vertiginoso desenvolvimento tecnológico no domínio da informática tem vindo a produzir um vastíssimo acervo de dispositivos e de bens informáticos, reclamando-se, neste domínio, a adoção de específicos instrumentos normativos.

Não obstante a expressão «bens informáticos» ([3]) venha sendo utilizada com um alcance mais abrangente, para a economia do parecer interessa convocar os elementos que compõem o sistema de *hardware*, nele se incluindo todos os componentes físicos de um computador (unidade de processamento central e dispositivos periféricos, assim como o designado *software*, cujo elemento principal e característico é um programa de computador ou um conjunto de programas de computador ([4]).

Tendo em conta o objeto da consulta, importa registar algumas considerações sobre o programa de computador, cuja noção a atual legislação portuguesa omite, mas que constava na designada lei da Criminalidade Informática, aprovada pela Lei n.º 109/91, de 7 de agosto, revogada pela Lei n.º 109/2009, de 15 de setembro, conhecida por «Lei do Cibercrime».

No artigo 2.º, alínea *c*), dessa lei, o programa informático era definido como «um conjunto de instruções capazes, quando inseridos num suporte explorável em máquina, de permitir à máquina que tem por funções o tratamento de informações, executar ou produzir determinada função, tarefa ou resultado».

Trata-se de uma noção próxima da que consta do Livro Verde da Comissão das Comunidades Europeias, de junho de 1988, sobre "O direito de autor e o desafio tecnológico". Neste documento, o programa de computador é definido como «um conjunto de instruções destinado a permitir que um dispositivo de tratamento da informação, um computador, execute as suas funções» ([5]).

O conceito de programa de computador não é totalmente coincidente com o de *software* embora seja o seu elemento principal e característico. A este propósito, tem-se entendido que o termo *software* assume uma maior amplitude que a expressão «programa de computador» na medida em que, como assinalam Garcia Marques e Lourenço Martins, «abrange um conjunto de programas e respetiva documentação», sendo esta constituída como «incluindo não só a preparatória como a que acompanha o fornecimento do programa ao utilizador e se designa por vezes de *manual do utilizador*, que pode ser apresentada em suporte de papel ou informático» ([6]).

José de Oliveira Ascensão, referenciando as orientações elaboradas pela Organização Mundial de Propriedade Intelectual (OMPI) em 1977, apresenta o *software* repartido em três categorias assim definidas:

«*a*) "Programa de Computador" é o conjunto de instruções capaz, quando incorporado num veículo legível pela máquina, de fazer com que uma máquina, que disponha de capacidade para processar informações, indique, desempenhe ou execute uma particular função, tarefa ou resultado;

b) "Descrição de Programa" é uma apresentação completa de um processo, expressa por palavras, esquemas ou de outro modo, suficientemente pormenorizada para determinar o conjunto de instruções que constitui o programa de computador correspondente;

c) "Material de Apoio" é qualquer material, para além do programa de computador e da descrição do programa, preparado para ajudar a compreensão ou a aplicação de um programa de computador, como por exemplo as descrições de programas e as instruções para usuários» ([7]).

Ultrapassado o tempo em que os fabricantes do *hardware* informático produziam o seu próprio *software*, utilizável apenas nos computadores que construíam (sistema de *bundling*), os programas de computador apresentam agora diferentes formatos ou tipos, consoante as instruções que contêm.

Numa perspetiva técnica ou funcional, podem referir-se os *programas base*, o *software* de base, operativo ou de sistema (por exemplo, os sistemas Windows ou Linux) e os *programas aplicativos* ou de utilidade. Os primeiros são essenciais ao funcionamento do computador, atuando como gestores de recursos do sistema, controlando as respetivas tarefas e a execução dos programas aplicativos, dando a estes um «ambiente» onde podem correr. Diferentemente dos sistemas operativos, as aplicações ou programas aplicativos são concebidos para a realização de determinadas tarefas pelos utilizadores (processadores de texto, folhas de cálculo, bases de dados, navegadores de Internet). Estão desenhados para a satisfação de necessidades específicas ou para a realização de determinadas tarefas do utilizador ([8]).

A partir do momento em que o *software* passou a ser desenvolvido e comercializado como produto autónomo dos computadores (processo de *unbundling*), surgiu a necessidade de conferir uma tutela jurídica específica «de modo a forçar, como salienta RUI SAAVEDRA, os potenciais interessados a obter licenças de utilização, cominando, simultaneamente, a ilicitude das cópias não autorizadas ([9]). Os utilizadores de computadores, prossegue o mesmo autor, «cedo se aperceberam da facilidade com que os programas de computador podiam ser copiados e objeto de permuta; pelas mesmas razões, alguns empresários, de idoneidade duvidosa, reconheceram que existia um mercado para o material copiado ilegalmente, que eles podiam facilmente satisfazer. Aqui ecoava o despertar para o fenómeno — que ainda hoje existe — da reprodução ilegítima de *software*, com uma mistura (complexa e afetando grandes valores económicos) de reprodução casual e de pirataria em larga escala» ([10]).

A *democratização da informática*, mais notória a partir dos anos 80 do século passado, e a penetração da tecnologia informática (difusão de microprocessadores e uso generalizado do computador pessoal) em âmbitos sociais cada vez mais vastos (escolas, serviços públicos e privados, pequenas e médias empresas, particulares) suscitou uma procura maciça de *software*, ocasionando um crescimento da oferta do mesmo.

Importantíssima criação específica da Informática, «o software representa, hoje, um valor económico muito significativo, ao ponto de ser já uma das mais poderosas indústrias à escala mundial» ([11]).

Constituindo um produto que pode facilmente ser reproduzido e ilimitadamente utilizável, o *software* tem sido objeto constante dos fenómenos de pirataria e plágio. Crê-se ser bastante significativa a percentagem de *software* pirateado. Neste sentido, pondera Rui Saavedra que «a indústria de *software* apresenta-se muito frágil e vulnerável economicamente, dada a facilidade de copiar o programa de computador rapidamente (em alguns minutos ou mesmo alguns segundos), a baixo custo (eventualmente apenas com o custo do suporte para onde é copiado, v. g. disquetes) — independentemente da autorização do seu criador ou titular —, com qualidade idêntica (por vezes até superior) à do original» ([12]).

Marie-Thérèse Huppertz dá conta de três das formas mais virulentas que a pirataria tem assumido no domínio da indústria de *software* que ilustram a séria ameaça que representa na era digital: (a) a cópia pelo utilizador final (*end-user copying*) ou «*corporate piracy*», a contrafação e a pirataria pela internet ([13]).

A propósito da primeira forma de pirataria, refere a autora citada que «os problemas mais graves da indústria de *software* têm envolvido tradicionalmente os seus utilizadores finais (*ultimate users*) — grandes ou pequenas organizações, empresas ou instituições públicas ou privadas — que compram um número inadequado de cópias e licenças de software, procedendo, em seguida, à sua cópia para utilização de um número excessivo de utilizadores. Neste tipo de pirataria, estamos perante cópias não autorizadas de *software* para computadores utilizados naquelas organizações sem a necessária aquisição de novas licenças. Esta forma de pirataria pode ser levada a cabo de forma individual, quando usuários individuais executam, por diversos meios, em suportes diversos, cópias não autorizadas ou licenciadas.

A contrafação no domínio do *software* constituirá talvez, segundo a mesma autora, a mais nociva forma de pirataria, uma vez que os desenvolvimentos tecnológicos têm possibilitado a réplica de um grande volume de *software* de modo fácil e barato. Esta forma de pirataria revela-se, nomeadamente, nos CD-ROMS que constituem réplicas em tudo idênticas aos produtos originais genuínos *(look alike CD-ROMS)* ([14]).

Expressando, enfim, o que constituirá entendimento comum, Miguel Moura e Silva sublinha que «os programas de computador são particularmente vulneráveis à reprodução através de meios técnicos pouco dispendiosos. O investimento na conceção e desenvolvimento dos programas de computador seria posto em causa se não fosse concedida proteção eficaz contra a sua reprodução» ([15]).

A simplicidade, o baixo custo e a eficácia da reprodução não autorizada de *software* explicam a sua natureza fortemente criminógena, a demandar formas mais intensas de tutela jurídica, em particular, a proteção penal.

Para além do recurso à proteção antiduplicação dos programas através de meios físicos ou técnicos a que muitos produtores de *software* recorrem ([16]), assume decisiva importância a demanda da sua proteção

jurídica, matéria que, de modo breve, tido por adequado ao objeto da consulta, examinaremos de seguida.

III

1 — O *software*, em particular o de tipo aplicacional, é um «bem complexo», suscetível de constituir objeto de múltiplas situações subjetivas ([17]), observando-se na doutrina uma multiplicidade de possíveis meios jurídicos de proteção: direito das patentes, das marcas, direito de autor, concorrência desleal, normas penais. Convocam-se também os institutos comuns do direito civil, tais como a responsabilidade civil e o direito dos contratos.

O debate que se gerou sobre os diversos esquemas normativos visando a proteção dos programas de computador veio a centrar-se no binómio: patentes de invenção — direito de autor, esgrimindo-se argumentos vários em defesa da opção por uma ou por outra destas vias.

Relativamente à proteção dos programas de computador pela via das patentes de invenção, invocava-se que eles tinham uma função essencialmente utilitária, sendo obras funcionais já que, afinal, se analisam, como já se disse, num conjunto de instruções que permite que um computador desempenhe certas funções ou alcançar determinados resultados ([18]). Nesta perspetiva, os programas de computador não constituirão, em rigor, qualquer expressão do génio criativo do seu autor.

Porém, como salienta Alexandre Dias Pereira, «o direito de autor é uma forma de propriedade intelectual sobre formas de expressão literária, artística e científica, criadas pelo espírito humano e exteriorizadas na forma de obras intelectuais», nada parecendo obstar, à partida «a que possa proteger também os programas de computador (ou *software*)». Com efeito, prossegue o autor, «os programas de computador são formas criativas no domínio da ciência, tendo em conta a expressão linguística em que se exprimem» ([19]).

2 — A economia do parecer dispensa tratamento mais desenvolvido sobre o dissenso doutrinal que se gerou relativamente ao meio ideal de proteção jurídica do *software* e dos programas de computador, na medida em que, diga-se desde já, a generalidade dos ordenamentos jurídicos adotou o direito de autor como a forma de propriedade intelectual mais adequada à prossecução dessa finalidade (de proteção) ([20]).

De facto, logo em 1973 foi celebrada em Munique a Convenção sobre a Patente Europeia ([21]), cujo artigo 52.º, n.º 1, exclui os programas de computador, enquanto tais, do catálogo das invenções suscetíveis de proteção pelo direito das patentes ([22]).

Em 1991, A Comunidade Europeia adotou a Diretiva 91/250/CEE do Conselho, de 14 de maio ([23]), relativa à proteção jurídica dos programas de computador, onde se determinou que «os Estados-membros estabelecerão uma proteção jurídica dos programas de computador, mediante a concessão de direitos de autor, enquanto obras literárias, na aceção da Convenção de Berna para a Proteção das Obras Literárias e Artísticas» (artigo 1.º, n.º 1).

Esta Diretiva foi revogada pela Diretiva 2009/24/CE do Parlamento Europeu e do Conselho ([24]), instrumento normativo que, no essencial, reproduz as disposições daquela.

Ainda no plano internacional, retenha-se que, em 1994, no âmbito do GATT, e durante o *Uruguay Round*, o Acordo sobre os Aspetos dos Direitos de Propriedade Intelectual Relacionados com o Comércio (ADPIC), também designado por Acordo TRIPS/ADPIC ([25]), e, em 1996, o Tratado sobre o Direito de Autor, celebrado sob a égide da OMPI, estabelece que os programas de computador serão protegidos enquanto obras literárias no sentido da Convenção de Berna.

De um modo geral, os Estados-membros da então Comunidade Europeia transpuseram a citada Diretiva 91/250/CEE, alterando as suas leis sobre o direito de autor por forma a abrangerem os programas de computador ([26]).

3 — Em Portugal, a transposição da Diretiva 91/250/CEE para o Direito interno operou-se, não através da alteração do regime jurídico do direito de autor, mas através da edição de diploma autónomo — o Decreto-Lei n.º 252/94, de 20 de outubro ([27]). Tratou-se de uma opção expressamente assumida pelo legislador no respetivo preâmbulo, onde se consigna que, «[d]e acordo com a melhor técnica decidiu-se criar um diploma próprio onde se condensem todas as normas específicas de proteção dos programas de computador, ao invés de se proceder a alterações no Código do Direito de Autor e dos Direitos Conexos».

O artigo 1.º, n.º 2, deste diploma atribui aos programas de computador «que tiverem caráter criativo», «proteção análoga à conferida às obras literárias» ([28]).

A expressão da norma parece significar, pondera Alexandre Dias Pereira, «que os programas de computador não são protegidos *tout court* enquanto obras literárias» ([29]). Como também se refere no preâmbulo do Decreto-Lei n.º 252/94, «os conceitos nucleares de proteção dos programas de computador transportam novas realidades que não são facilmente subsumíveis às existentes no direito de autor, muito embora a equiparação a obras literárias possa permitir, pontualmente, uma aproximação».

Segundo este autor, a *proteção análoga* à conferida às obras literárias «traduz-se num regime jurídico nuclearmente *sui generis*, análogo à tutela jurídico-autoral, radicado na concessão de direitos de autor *anómalos*» ([30]).

A este propósito, salienta José Alberto Vieira que, «[n]um posicionamento de inequívoca relutância, melhor, de verdadeira rejeição da qualificação, a lei portuguesa não dispõe que os programas de computador são obras literárias, como determina o artigo 1.º, n.º 1, da Diretiva 91/250/CEE. Ao invés, preceitua que "é atribuída proteção análoga"» ([31]). Todavia, segundo o mesmo autor, parece não ter sido instituído um regime "*sui generis*", já que «o regime jurídico constante do Decreto-Lei n.º 252/94 assenta totalmente no paradigma do direito de autor» ([32]).

O objeto do parecer dispensa considerações mais desenvolvidas também sobre esta questão, interessando, no entanto, convocar as normas contidas nos artigos 13.º e 14.º do Decreto-Lei n.º 252/94, relativas à apreensão e à tutela penal, respetivamente ([33]).

O artigo 13.º, n.º 1, dispõe que se aplicam à apreensão de cópias ilícitas de programas de computador as disposições relativas à apreensão de exemplares contrafeitos em matéria de direito de autor».

As disposições do Código do Direito de Autor e dos Direitos Conexos (CDADC) ([34]) mobilizáveis, por força da expressa remissão contida naquele preceito, constam dos n.os 1 e 2 do seu artigo 201.º, integrado no Título IV dedicado à violação e defesa do direito de autor e dos direitos conexos, cujo teor interessa conhecer:

«Artigo 201.º

Apreensão e perda de coisas relacionadas com a prática do crime

1 — São sempre apreendidos os exemplares ou cópias das obras usurpadas ou contrafeitas, quaisquer que sejam a natureza da obra e a forma de violação, bem como os respetivos invólucros materiais, máquinas ou demais instrumentos ou documentos de que haja suspeita de terem sido utilizados ou de se destinarem à prática da infração.

2 — Nos casos de flagrante delito, têm competência para proceder à apreensão as autoridades policiais e administrativas, designadamente a Polícia Judiciária, a Polícia de Segurança Pública, a Polícia Marítima, a Guarda Nacional Republicana, a Autoridade de Segurança Alimentar e Económica e a Inspeção-Geral das Atividades Culturais.»

Por sua vez, estipula o citado artigo 14.º do Decreto-Lei n.º 252/94:

«Artigo 14.º

Tutela penal

1 — Um programa de computador é penalmente protegido contra a reprodução não autorizada.

2 — É aplicável ao programa de computador o disposto no n.º 1 do artigo 9.º da Lei n.º 109/91, de 17 de agosto.»

Como já se disse, a proteção jus autoral dos programas de computador não exclui a aplicação de outras formas de proteção. Assim o artigo 15.º do Decreto-Lei n.º 252/94 estabelece expressamente que a tutela que institui «não prejudica a vigência de regras de diversa natureza donde possa resultar uma proteção do programa, como as emergentes da disciplina dos direitos de patente, marcas, concorrência desleal, segredos comerciais e das topografias dos semicondutores ou do direito dos contratos».

IV

1 — De acordo com o disposto na alínea *a*) do artigo 4.º da Diretiva 91/250/CEE, no direito exclusivo do titular do programa de computador está incluído o direito de autorizar:

«*a*) A reprodução permanente ou transitória de um programa de computador, seja por que meio for, e independentemente da forma de que se revestir, no todo ou em parte. Se operações como o carregamento, visualização, execução, transmissão ou armazenamento de um programa de computador carecerem dessa reprodução, essas operações devem ser submetidas a autorização do titular do direito» ([35]).

Em correspondência com esta disposição, estabelece o artigo 5.º, alínea *a*), do Decreto-Lei n.º 252/94, que o titular do programa de computador pode autorizar «a reprodução, permanente ou transitória, por qualquer processo ou forma, de todo ou de parte do programa».

Segundo Miguel Moura e Silva, «o mais importante direito exclusivo de natureza patrimonial atribuído ao autor é o direito à reprodução da obra. É aliás neste direito que assenta o regime anglo-saxónico do "*copyright*". Devido às circunstâncias particulares em que ocorre, é comum

entender que a utilização de um programa de computador envolve a reprodução do mesmo. Para que possa desempenhar a função a que se destina, fornecer ao computador as instruções necessárias para a prossecução de determinada tarefa, o programa de computador deve ser previamente introduzido no computador, designadamente mediante o seu armazenamento na memória do computador (carregamento ou "loading")» ([36]).

A produção de novos exemplares de um programa informático em suportes corpóreos duradouros representa sempre uma reprodução, sendo indiferente o tipo de suporte no qual a cópia é feita: disco rígido, disquetes, CD, banda magnética ou outro. Como salienta José Alberto Vieira, «desde a simples operação de "*downloading*" de um programa da Internet para o disco rígido do computador ou para uma disquete, à sofisticada produção de CD ROMs numa linha de fabrico industrial ou à transmissão em "*routing*" numa rede de computadores, todos estes processos de multiplicação do programa se encontram abrangidos pelo poder de reprodução reconhecido ao titular do direito patrimonial de autor» ([37]).

2 — O artigo 14.º do Decreto-Lei n.º 252/94, acima reproduzido, consagra uma tutela penal dos programas de computador contra a sua reprodução não autorizada, remetendo para o n.º 1 do artigo 9.º da Lei n.º 109/91, de 17 de agosto — lei da criminalidade informática.

Nos termos deste preceito:

«Artigo 9.º

Reprodução ilegítima de programa protegido

1 — Quem, não estando para tanto autorizado, reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei será punido com pena de prisão até três anos ou com pena de multa.

2 — . . . . . .

3 — A tentativa é punível.»

O legislador considerou, pois, os programas de computador como bens dignos de merecerem tutela penal, sancionando os atos de reprodução não autorizada ([38]).

O interesse que se visa proteger com a incriminação desta conduta é, essencialmente, a propriedade intelectual — o direito de autor, já que se visa garantir ao titular dos direitos de criação dos programas o uso dos mesmos, mediante autorização (e remuneração).

Como escreve Benjamim Silva Rodrigues, visa proteger-se «o exclusivo de exploração (-) (económica) de um específico fluxo informativo-comunicacional exteriorizável e materializável num determinado suporte eletrónico-digital, criativo, genuíno e íntegro (-), inovador e original (ou equiparado) fruto da criação ou invenção intelectual de uma determinada pessoa humana e parte integrante do património do seu originário ou derivado titular» ([39]).

Segundo o mesmo autor:

«A principal e primacial ideia rectora deste tipo legal de crime prende-se com o combate à pirataria informática (-) ou do "*software*" que surge como um flagelo característico da Sociedade Informacional e Comunicacional dos nossos dias. Pretende-se evitar que aquele específico fluxo informativo-comunicacional funcional extravase a zona de exclusividade e domínio do seu legítimo autor e criador sem a sua autorização e ou conhecimento, causando uma diminuição ou prejuízo patrimonial do seu titular» ([40]).

3 — A Lei n.º 109/91 foi revogada pela Lei n.º 109/2009, de 15 de setembro, que aprovou a lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, adotada em Budapeste em 23 de novembro de 2001 ([41]).

Em termos sistemáticos, este diploma compõe-se de cinco capítulos que versam, sucessivamente, sobre:

Capítulo I — Objeto e definições;
Capítulo II — Disposições penais materiais;
Capítulo III — Disposições processuais;
Capítulo IV — Cooperação internacional; e
Capítulo V — Disposições finais e transitórias.

4 — O capítulo I da lei enuncia o seu objeto e apresenta um conjunto de definições. Neste domínio, terá interesse atentar que, para efeitos do diploma, considera-se *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, proteção e manutenção» — artigo 2.º, alínea *a*).

Por *dados informáticos*, entende-se «qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função» — artigo 2.º, alínea *b*).

Como salienta Pedro Verdelho, o conceito de «dados informáticos» introduzido por este diploma, «pretende vir a substituir o antigo conceito, de âmbito mais reduzido, mais limitado e atualmente tecnicamente desajustado, de programa informático (que constava da alínea *c*) do artigo 2.º da Lei n.º 109/91) ([42]). «É pacífico assumir, prossegue o autor, que um programa informático é composto por dados informáticos, mas nem todos os dados informáticos integram um programa. Todavia, estes dados, que não consubstanciam um programa, podem também ser objeto de uma ação humana lesiva dos interesses de outrem, a qual merece tutela penal. Por isso, a lei optou por criar o conceito legal de dados informáticos, nele se incluindo o outro, ontologicamente de menor dimensão, de programa informático» ([43]).

5 — No capítulo dedicado às *disposições penais materiais*, estão previstos os crimes de falsidade informática (artigo 3.º), de dano relativo a programas ou outros dados informáticos (artigo 4.º), de sabotagem informática (artigo 5.º), de acesso ilegítimo a um sistema informático (artigo 6.º), de interceção ilegítima de transmissões de dados informáticos (artigo 7.º) e, por fim, o crime de reprodução ilegítima de programa protegido (artigo 8.º).

6 — Integrando o objeto da consulta, interessa conhecer a descrição típica do crime de *reprodução ilegítima de programa protegido* acolhida no artigo 8.º, n.º 1, da lei do Cibercrime:

«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 3 anos ou com pena de multa.

2 — . . . . . .

3 — A tentativa é punível.»

Esta norma corresponde à contida no artigo 9.º, n.º 1, da Lei n.º 109/91 (Lei da Criminalidade Informática), sendo, no essencial, coincidente o conteúdo semântico das duas disposições.

São elementos típicos deste crime, cuja tentativa é punível, conforme dispõe o n.º 3 do artigo 8.º, (*a*) a falta de autorização; (*b*) a ação — reproduzir, divulgar ou comunicar ao público; (*c*) o objeto da ação — o programa informático protegido por lei ([44]); e (*d*) o dolo.

Oportunamente já se referenciou ([45]) que o conceito de reprodução envolve quer «a simples operação de "*downloading*" de um programa da Internet para o disco rígido do computador ou para uma disquete», quer a produção de CD-ROMs ou de outros dispositivos ou suportes externos, amovíveis e tangíveis, quer a «transmissão em "*routing*" numa rede de computadores». Trata-se de duplicação ou multiplicação de programas informáticos que «se encontram abrangidos pelo poder de reprodução reconhecido ao titular do direito patrimonial de autor» ([46]).

A norma constante do artigo 8.º, n.º 1, acima transcrita, define como crime *qualquer tipo de reprodução não autorizada* de um programa informático. Como sublinha Pedro Verdelho, «o mero ato de fazer uma cópia de um programa informático para um suporte autónomo de dados (CD ROM, *pen disks*, disco rígido ou outro suporte de dados), ou para o instalar num computador, é proibido e punido por lei» ([47]).

A respeito do conceito de reprodução, a doutrina maioritária (segundo cremos) vem considerando que a prática deste crime ocorre quando o agente execute quer uma operação de duplicação ou multiplicação física do programa, quer proceda à sua fixação ou memorização em computador ([48]).

Por outro lado, tem-se entendido que os elementos contemplados no n.º 1 do artigo 8.º (reprodução, divulgação, comunicação ao público) não são cumulativos, bastando, para a verificação do crime, a simples reprodução ilegítima do *software*.

A jurisprudência portuguesa tem acolhido o conceito de reprodução para efeitos penais que se indicou ([49]).

7 — O tratamento devido às questões suscitadas nesta consulta impõe que se teçam algumas considerações sobre o conceito de *criminalidade informática* e sua caracterização.

Embora a sua definição não se encontre uniformemente sedimentada na doutrina, consideram Garcia Marques e Lourenço Martins ser «frequente encarar a criminalidade informática como todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo simbólico desse ato ou em que o computador é "objeto" do crime» ([50]), ou, de modo mais analítico, como «qualquer atividade criminal que envolva a cópia, o uso, a transferência, a interferência, o acesso ou a manipulação de sistemas de computador, de funções de computador, de dados ou programas de computador» ([51]).

Pedro Verdelho alude aos crimes que, não obstante cometidos por via de computadores ou sistemas de computadores, «não se distinguem do mesmo tipo de crime cometido por outras vias. Embora sejam crimes cometidos *on line*, isso não lhes confere nenhuma especialidade. Dogmaticamente nada os distingue da sua forma tradicional, apenas tendo de diferente o meio usado» ([52]). «Destes se distinguem outros crimes — prossegue o mesmo autor — que têm de especial o ambiente em que são praticados. Não poderiam ser cometidos noutro meio nem por outro meio. São gerados no ambiente informático e só podem ocorrer pela especificidade do meio».

Ainda segundo o mesmo autor, há uma outra espécie de crimes que se caracterizam «por serem praticados contra o meio informático. São crimes contra computadores ou sistemas de computadores. São os crimes informáticos propriamente ditos» ([53]).

Numa outra tipologia, nos «crimes relacionados com a informática» podem identificar-se «*crimes que recorrem a meios informáticos*», ilícitos «que só podem ser cometidos com o recurso a meios informáticos, mas que dogmaticamente não se distinguem dos crimes tradicionais», como sucede nos crimes informáticos previstos no Código Penal (burla informática — artigo 221.º — e devassa por meio de informática — artigo 193.º).

E podem apontar-se também os designados «*crimes informáticos propriamente ditos*», correspondentes àqueles «cujo objeto e instrumento de execução é a informática, são praticados através da informática e contra elementos informáticos» e que «são essencialmente os constantes na lei da Criminalidade Informática (LCI)» ([54]).

Neste âmbito, outro autor distingue entre «crimes tipicamente informáticos», «crimes essencialmente informáticos» e «crimes acidentalmente informáticos» ([55]).

Os crimes essencialmente informáticos são aqueles «em que o próprio bem jurídico ofendido consiste numa realidade informática com dignidade suficiente para merecer a tutela penal» ([56]), como sucede, precisamente, no caso da reprodução ilegítima de programa informático.

O crime informático constituirá, pois, uma infração que pressupõe necessariamente a utilização do computador e da tecnologia informática para a sua prática. O crime só pode executar-se através da informática.

Neste contexto, Jaime Nuno da Silva Fernandes considera que este crime pode ser definido como «todo o ato considerado ilícito, cometido por via do recurso à tecnologia informática, cujas características específicas são intencionalmente procuradas e ou aproveitadas pelo agente» ([57]).

A «contrafação de *software*» constitui, para este autor, precisamente uma das modalidades de crime informático ([58]).

Dos elementos doutrinários recenseados, pode concluir-se, sem hesitação, que o crime de reprodução ilegítima de programa protegido configura um autêntico crime informático, com a ação delituosa a ser levada a cabo utilizando um meio ou objeto informático, no caso, o *software*. A tecnologia informática é essencial para a sua execução.

O legislador português assim o reconhece, tipificando a reprodução ilícita ou ilegítima de programa de computador como crime informático, tanto na Lei n.º 109/91 (Lei da Criminalidade Informática), como, presentemente, na lei do Cibercrime.

A propósito deste delito, e numa perspetiva sociocriminal, dá conta Pedro Verdelho que a reprodução ilícita de programa protegido chegou a constituir «o grupo numericamente mais significativo de casos» de crimes informáticos, acrescentando que, «[e]m meados da década de 1990 traduziam maioritariamente uma de duas realidades: ou a venda em locais públicos (*maxime* a Feira da Ladra e lojas de venda de material informático) ou a deteção ocasional de *software* ilicitamente instalado em locais de acesso privado (escritórios, empresas) no decurso de ações de fiscalização administrativa, fiscal ou outra» ([59]).

Não obstante muita da reprodução ilícita de programas se operar atualmente através de *downloads* da Internet, crê-se que se continuarão a comercializar um significativo número de programas «pirateados», no sentido de objeto de contrafação, contidos em suportes autónomos ou amovíveis, assim como será recorrente a prática censurável da instalação e utilização ilícita de programas em computadores ou em sistemas informáticos.

A proteção penal concedida aos direitos, fundamentalmente económicos, dos autores de programas de computador é, neste conspecto, perfeitamente justificada, sem prejuízo, como já se disse, e como expressamente estabelece o Decreto-Lei n.º 252/94 (artigo 15.º), da tutela conferida por regras jurídicas de diversa natureza ([60]).

V

1 — O Capítulo III da lei do Cibercrime versa sobre *disposições processuais* aplicáveis, designadamente, aos crimes que tipifica.

Assim, sobre o seu âmbito, dispõe o artigo 11.º que:

«Artigo 11.º

Âmbito de aplicação das disposições processuais

1 — Com exceção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:

a) Previstos na presente lei;
b) Cometidos por meio de um sistema informático; ou
c) Em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

2 — As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de julho [([61])].»

A Lei n.º 109/2009 (Lei do Cibercrime) «condensou num só diploma legislativo todas as normas respeitantes à cibercriminalidade, aglutinando normas de direito penal material (sobretudo criando tipos de crime), normas processuais (que são exceções às regras gerais do Código de Processo Penal) e ainda normas respeitantes à cooperação penal internacional» ([62]).

Refira-se, como também o autor que se vem citando consigna, que esta Lei não introduziu inovações de relevo aos tipos de crime já descritos na lei da Criminalidade Informática (Decreto-Lei n.º 109/91). «Já quanto às normas de direito processual penal a inovação foi bastante maior, passando a ordem jurídica portuguesa a prever normas processuais específicas, neste domínio» ([63]).

Na economia do parecer interessa conhecer as normas processuais contemplada nesta lei, impondo-se uma particular atenção ao regime da pesquisa e da apreensão de dados informáticos definido nos artigos 15.º e 16.º, respetivamente.

2 — Pese embora a sua extensão, afigura-se-nos útil transcrever os artigos 12.º a 17.º deste diploma que dispõem, respetivamente, sobre a preservação expedita de dados, a revelação expedita de dados de tráfego, a injunção para apresentação ou concessão do acesso a dados, a pesquisa de dados informáticos, a apreensão de dados informáticos e a apreensão de correio eletrónico e registos de comunicações de natureza semelhante.

«Artigo 12.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, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5 — A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do n.º 3, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 13.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 efetuada, tendo em vista

permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efetuada.

Artigo 14.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 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 faturação 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, das atividades médica e bancária e da profissão de jornalista.

7 — O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Artigo 15.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 e no Estatuto do Jornalista.

Artigo 16.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 efetuar 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 suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo 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 efetuadas 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 atividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista.

6 — O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

7 — 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 respetiva 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.

8 — No caso da apreensão efetuada nos termos da alínea *b*) do número anterior, a cópia é efetuada 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 17.º

Apreensão de correio eletrónico 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 eletrónico 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.»

3 — Como já se disse, estas disposições consagram um regime processual específico para as investigações das infrações criminais previstas nesta lei, assim como dos crimes cometidos por meio de um sistema informático e ainda dos crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (cf. artigo 11.º, n.º 1).

O legislador reconheceu, conforme se lê na exposição de motivos da Proposta de Lei n.º 289/X/4.ª, iniciativa que esteve na base da lei do Cibercrime ([64]), que «no campo das normas de direito processual penal, a desadequação da ordem jurídica nacional às novas realidades a implementar é superior» à que se verifica no domínio do direito penal substantivo.

Recordando que no conceito de dados informáticos, definido na alínea *b*) do artigo 2.º da Lei n.º 109/2009, cabem os programas informáticos, todos os novos meios de obtenção de prova, consagrados neste

diploma, podem ser convocados na investigação do crime de reprodução ilegítima de programa protegido, previsto e punido no seu artigo 8.º

As inovadoras medidas processuais de preservação expedita de dados armazenados num computador e de preservação expedita e revelação de dados de tráfego foram introduzidas em cumprimento das obrigações resultantes dos artigos 16.º e 17.º da Convenção sobre o Cibercrime do Conselho da Europa. São medidas essenciais para a eficácia das investigações criminais no domínio digital. A rapidez na preservação de dados é imprescindível a qualquer investigação, pois, se tal não suceder, os dados perder-se-ão.

Como decorre do n.º 1 do artigo 12.º da lei do Cibercrime, a medida de *preservação expedita de dados* pressupõe que já esteja instaurado um processo de investigação do crime. Recorre-se a ela quando, *no decurso do processo*, a autoridade judiciária competente (Ministério Público, juiz de instrução ou juiz do julgamento) entenda que é necessária, tendo em vista a descoberta da verdade.

A preservação também pode ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no CPP onde se mencionam, de forma resumida, o que se executou, o que se apurou e as provas obtidas.

Foi introduzido e regulado o mecanismo da injunção, inspirado no artigo 18.º da Convenção sobre o Cibercrime. Sobre a justificação desta medida, refere Pedro Verdelho que «as razões que lhe estão subjacentes prendem-se com a efetiva dificuldade, sentida por quem investiga, no acesso a informação, quando esta está armazenada em sistemas informáticos, sobretudo em consequência da grande capacidade de armazenamento dos sistemas modernos e da sua enorme complexidade. Na verdade, por um lado, na imensidade de espaço de armazenamento dos modernos suportes digitais, pode ser muito difícil e moroso encontrar a informação que se pretende se não se contar com a colaboração de quem tem disponibilidade sobre o sistema [...]. Por outro lado, as diversas possibilidades de ocultar a informação ou de bloquear o acesso [...] podem tornar mal sucedida a procura de informação, sem a colaboração de quem tem o domínio sobre ela» ([65]).

A medida da injunção é aplicável, havendo processo instaurado, como decorre da expressão «decurso do processo», e se se revelar necessária para a descoberta da verdade.

4 — A matéria da busca e apreensão de dados armazenados num computador está prevista no artigo 19.º da Convenção sobre o Cibercrime e regulada nos artigos 15.º a 17.º da Lei n.º 109/2009.

Tendo presente o teor da exposição da entidade que solicitou a intervenção deste corpo consultivo, interessa examinar, com mais detalhe, o regime definido para a pesquisa de dados informáticos, medida prevista no artigo 15.º, e para a apreensão de dados informáticos, contemplada no artigo 16.º

A essência destas medidas processuais coincide, no ambiente do ciberespaço, com as formas clássicas de busca e apreensão desenhadas nos artigos 174.º e 178.º do Código de Processo Penal (CPP). No entanto, como se aponta na Exposição de motivos da Proposta de Lei n.º 289/X, «a forma como a busca e a apreensão estão descritas no Código de Processo Penal exigiam alguma adequação a estas novas realidades».

4.1 — A *pesquisa de dados informáticos* num sistema informático conserva, como lembra Paulo Dá Mesquita, «a sua verdadeira natureza processual de busca», acrescentando que:

> «Apesar da originalidade terminológica da lei do cibercrime, continuam a valer os cânones estabelecidos no artigo 174.º, n.º 1, do CPP, pelo que: 1. Quando houver indícios de que dados informáticos relacionados com um crime ou que possam servir de prova se encontram num determinado sistema informático é ordenada a busca informática; 2. A busca informática é ordenada por despacho pela autoridade judiciária competente, devendo esta, sempre que possível, presidir à diligência» ([66]).

De acordo com o disposto no n.º 1 do artigo 15.º da lei do Cibercrime, a pesquisa de dados informáticos específicos e determinados armazenados num sistema informático pressupõe também que esteja pendente um processo, no decurso do qual ela se revele necessária, tendo em vista a descoberta da verdade.

A medida depende de autorização da autoridade judiciária competente que, sempre que possível, deverá presidir à diligência.

O n.º 3 do mesmo preceito enuncia as situações em que o órgão de polícia criminal pode proceder à pesquisa sem prévia autorização da autoridade judiciária: quando for consentida voluntariamente por quem tiver a disponibilidade ou controlo dos dados [alínea *a*)], ou 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 [alínea *b*)]. Nesta última situação, a realização da diligência deverá ser, sob pena de nulidade, imediatamente comunicada à autoridade judiciária para efeitos de apreciação e validação [n.º 4, alínea *a*)].

O n.º 5 do mesmo preceito prevê que quando no decurso de pesquisa a um sistema de computadores surgirem razões para crer que os dados que se procuram se encontram alojados noutro sistema informático, a busca pode ser estendida a outro sistema mediante autorização ou ordem da autoridade judiciária competente.

4.2 — Relativamente à *apreensão de dados informáticos*, também «não se alteram — segundo o autor que vimos acompanhando — os pressupostos funcionais da apreensão em processo penal (cf. artigo 178.º, n.os 1 e 3, do CPP), pelo que: 1. São apreendidos os sistemas informáticos e os dados informáticos que tiverem servido ou estivessem destinados a servir a prática de um crime, e bem assim todos aqueles que tiverem sido deixados pelo agente no local do crime ou quaisquer outros suscetíveis de servir de prova; 2. As apreensões de sistemas e dados informáticos são autorizadas, ordenadas ou validadas por despacho da autoridade judiciária» ([67]).

Á semelhança do que se prevê no artigo 178.º, n.º 4, do CPP, o artigo 16.º, n.º 2, da lei do Cibercrime permite que o órgão de polícia criminal efetue apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática a um sistema informático legitimamente ordenada, bem como quando haja urgência ou perigo na demora. As apreensões efetuadas nestas circunstâncias são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas (n.º 4 do mesmo preceito).

Por seu lado, o n.º 3 do mesmo preceito estabelece a obrigatoriedade de intervenção do juiz de instrução no caso de serem apreendidos dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro. Nestas situações, esses dados ou documentos serão apresentados ao juiz, sob pena de nulidade, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

Trata-se de um regime desenhado com vista à salvaguarda da intimidade e da privacidade do titular dos dados ou documentos informáticos, ou de terceiro, valores constitucionalmente garantidos (artigo 35.º da Constituição da República). A lei «parece não ignorar que, cada vez mais, os cidadãos guardam nos seus computadores pessoais documentos escritos, fotografias, filmes ou gravações sonoras que são suscetíveis de revelar segredos e que são manifestações da vida íntima ou privada do seu dono» ([68]).

O n.º 7 do artigo 16.º desta lei contempla as formas que a apreensão de dados informáticos pode revestir. Elas variarão de acordo com os interesses e as necessidades da investigação que se fizerem sentir no caso concreto, tendo em atenção os princípios da adequação e da proporcionalidade, podendo assumir uma das modalidades enunciadas nas suas alíneas *a*), *b*), *c*), e *d*):

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 respetiva 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.

5 — Foi dito que a essência destas medidas processuais coincide, no ambiente do ciberespaço, com as formas clássicas de busca e apreensão previstas nos artigos 174.º e 178.º do Código de Processo Penal.

Prescindindo o parecer de considerações mais desenvolvidas sobre a temática das buscas e apreensões, tendo em conta a disciplina consagrada nos artigos 15.º e 16.º da lei do Cibercrime, importa recordar que as *buscas* se fundamentam sempre numa suspeita de que objetos relacionados com um crime ou que possam servir de prova se encontram em certo lugar reservado ou não livremente acessível ao público (artigo 174.º, n.º 2, do CPP).

No domínio dos *poderes cautelares dos órgãos de polícia criminal* quanto aos meios de prova, interessa também convocar o artigo 251.º, n.º 1, alínea *a*), do CPP, que admite que aqueles podem proceder, sem prévia autorização da autoridade judiciária, a buscas no lugar em que o suspeito se encontrar, salvo tratando-se de busca domiciliária, sempre que tiverem fundada razão para crer que aí se ocultam objetos relacionados com o crime, suscetíveis de servirem a prova e que de outra forma se poderiam perder.

As apreensões, que se distinguem da busca, mas que se lhe acham associadas, muitas vezes sequencialmente, destinam-se a recolher e fazer juntar ao processo como meio de prova, os objetos que tiverem servido para a prática da infração ou que constituírem o seu produto, lucro, preço ou recompensa, e bem assim todos os objetos que tiverem sido deixados pelo agente no local ou quaisquer outros suscetíveis de servir de prova (artigo 178.º, n.º 1, do CPP), sendo ordenadas ou validadas pela autoridade judiciária competente (n.º 3 do mesmo preceito).

Os órgãos de polícia criminal podem efetuar apreensões no decurso de revistas ou de buscas ou quando haja urgência ou perigo na demora (n.º 4 do artigo 178.º do CPP) ([69]).

6 — Tendo em consideração o quadro normativo apresentado e os elementos da doutrina coligidos, estaremos em condições para responder à primeira questão suscitada pela ASAE. Trata-se, essencialmente, da questão de saber se as disposições processuais previstas nos artigos 12.º a 17.º da lei do Cibercrime são aplicáveis à investigação do crime de reprodução ilegítima de programa protegido tipificado no n.º 1 do artigo 8.º do mesmo diploma.

A resposta não pode deixar de ser afirmativa. Como se disse, este ilícito criminal assume a natureza de crime informático e como tal tipificado na Lei do Cibercrime. Tendo presente o conceito de dados informáticos, no qual também se integram os programas de computador, não restarão dúvidas de a prática deste crime envolver a utilização de um sistema informático ([70]). Consequentemente, as normas processuais contidas nos citados preceitos desse diploma podem e devem, quando necessário e verificados os respetivos pressupostos, ser convocadas no âmbito da sua investigação e perseguição criminal. Assim expressamente dispõe o artigo 11.º, n.º 1, alíneas *a*) e *b*), da Lei n.º 109/2009.

Tendo em conta a multiplicidade e plasticidade das formas e das circunstâncias em que este crime pode ser cometido, o recurso às disposições processuais privativas da Lei do Cibercrime variará, naturalmente, em função dos interesses e das necessidades da investigação que se fizerem sentir no caso concreto, tendo sempre em atenção, reafirma-se, os princípios da adequação e da proporcionalidade e a descoberta da verdade.

VI

1 — No pedido de intervenção deste Conselho suscita-se ainda a questão da competência da ASAE para investigar o crime de reprodução ilegítima de programa protegido, tendo presente que, de acordo com o disposto na alínea *l*) do n.º 3 do artigo 7.º da Lei n.º 49/2008, de 27 de agosto, que aprova a Lei de Organização da Investigação Criminal (LOIC), é da competência reservada da Polícia Judiciária a investigação dos crimes informáticos e praticados com recurso a tecnologia informática. Assim, afirma-se, «torna-se essencial apurar, com rigor, em que moldes a ASAE deve atuar no âmbito da Lei n.º 109/2009, de 15 de setembro».

2 — A direção do inquérito cabe ao Ministério Público, assistido pelos órgãos de polícia criminal, conforme se dispõe no artigo 263.º, n.º 1, do CPP. Neste âmbito, os órgãos de polícia criminal atuam sob a direta orientação do Ministério Público e na sua dependência funcional (n.º 2 do mesmo preceito).

Os órgãos de polícia criminal, de acordo com a definição contida na alínea *c*) do artigo 1.º do Código de Processo Penal (CPP), são «todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer atos ordenados por uma autoridade judiciária ou determinados por este Código».

Segundo Germano Marques DA Silva, os órgãos de polícia criminal «não são senão os órgãos das diversas corporações de polícia enquanto exercem a polícia criminal» ([71]), que define como a «atividade dos vários órgãos de polícia enquanto tem por objeto atos processuais ordenados por uma autoridade judiciária ou diretamente determinados pela lei processual penal» ([72]).

Tratando da delimitação do conceito de órgão de polícia criminal, Paulo Dá Mesquita refere que «a lei processual, ao invés de operar uma definição fechada de órgãos de polícia criminal, procedeu a um reenvio aberto que tem por referente a repartição clássica entre funções de polícia judiciária e polícia administrativa, pois "a caracterização é de ordem finalística: a polícia judiciária é uma atividade auxiliar quando levada a cabo pela Administração Pública"» ([73]). Para este Autor, se o conceito de autoridade judiciária está limitado no CPP [artigo 1.º, alínea *b*)], e o de autoridade de polícia criminal «tem de ser completado pelas leis orgânicas dos órgãos de polícia criminal» [artigo 1.º, alínea *d*)], «o conceito de órgão de polícia criminal é aberto e tem de ser completado pelas leis orgânicas ou estatutos dos diferentes organismos (secretarias judiciais, polícias, inspeções-gerais, outras entidades públicas a quem seja reconhecida competência para levar a cabo "quaisquer atos ordenados por uma autoridade judiciária ou determinados pelo CPP")» ([74]).

Na mesma linha, se bem vemos, José Manuel Damião da Cunha, considera que o conceito de "órgão de polícia criminal" do CPP «traduz a ideia de que o que releva é, não a qualidade do órgão/agente que pratica o ato, mas sim o tipo de ato ou atividade que é realizado. Isto que, do ponto de vista do CPP, é uma solução coerente, não significa, nem poderia significar, que o grau e a qualidade de intervenção e a ligação das diversas polícias às autoridades judiciárias sejam sempre os mesmos ([75]). Com efeito, prossegue o Autor, «o grau de ligação (embora sempre funcional) dependerá de outras questões, nomeadamente do tipo de criminalidade que cada polícia processa ou então da competência que lhe é atribuída» ([76]) ([77]).

Este entendimento encontra-se acolhido na lei de organização da investigação criminal, aprovada pela Lei n.º 49/2008, de 27 de agosto, cujo artigo 3.º dispõe que são órgãos de polícia criminal de *competência genérica*: (*a*) a Polícia Judiciária; (*b*) a Guarda Nacional Republicana; e (*c*) a Polícia de Segurança Pública (n.º 1), sendo órgãos de polícia criminal de *competência específica* todos aqueles a quem a lei confira esse estatuto (n.º 2), como sucede com a ASAE.

3 — A Autoridade de Segurança Alimentar e Económica (ASAE) foi criada pelo Decreto-Lei n.º 237/2005, de 30 de dezembro, em resultado da extinção de diversos serviços ([78]), e a sua orgânica atual consta do Decreto-Lei n.º 274/2007, de 30 de julho ([79]).

A ASAE — afirma-se no preâmbulo deste diploma — «congrega num único organismo a quase totalidade dos serviços relacionados com a fiscalização e com a avaliação e comunicação dos riscos na cadeia alimentar, com significativos ganhos de eficiência e maior eficácia, procedendo a uma avaliação científica independente dos riscos na cadeia alimentar e fiscalizando as atividades económicas a partir da produção e em estabelecimentos industriais ou comerciais».

Nos termos do artigo 1.º do Decreto-Lei n.º 237/2005, a ASAE é um serviço central da administração direta do Estado dotado de autonomia administrativa e dispõe de unidades orgânicas desconcentradas de âmbito regional, designadas direções regionais.

A jurisdição territorial da ASAE está definida no artigo 2.º: enquanto entidade nacional responsável pela avaliação e comunicação dos riscos na cadeia alimentar e autoridade coordenadora do controlo oficial dos géneros alimentícios, tem âmbito nacional (n.º 1); enquanto entidade fiscalizadora das atividades económicas, a ASAE exerce a sua atividade em todo o território do continente (n.º 2); no âmbito da fiscalização das atribuições das alíneas *p*) e *aa*) do n.º 2 do artigo 3.º, a ASAE exerce a sua atividade em todo o território nacional (n.º 3).

Nos termos do disposto no artigo 3.º, n.º 1, a ASAE «tem por missão a avaliação e comunicação dos riscos na cadeia alimentar, bem como a fiscalização e prevenção do cumprimento da legislação reguladora do exercício das atividades económicas nos setores alimentar e não alimentar, exercendo funções de autoridade nacional de coordenação do controlo oficial dos géneros alimentícios e organismo nacional de ligação com outros Estados membros».

No campo das suas atribuições, enunciadas no n.º 2 do mesmo preceito, interessa, na ótica da consulta, destacar as previstas nas suas alíneas *s*), *t*) e *ab*). Assim, constituem atribuições da ASAE:

> «*s*) Fiscalizar o cumprimento das obrigações legais dos agentes económicos;
>
> *t*) Fiscalizar todos os locais onde se proceda a qualquer atividade industrial, comercial, agrícola, pecuária, de abate, piscatória, incluindo a atividade de pesca lúdica, de promoção e organização de campos de férias, ou de prestação de serviços, designadamente de produtos acabados e ou intermédios, armazéns, escritórios, meios de transporte, entrepostos frigoríficos, empreendimentos turísticos, empreendimentos de turismo no espaço rural, estabelecimentos de turismo de natureza, agências de viagens, empresas de animação turística, estabelecimentos de restauração e bebidas, cantinas e refeitórios, clínicas dentárias, clínicas veterinárias, recintos de diversão ou de espetáculos, infraestruturas, equipamentos, espaços desportivos, portos, gares e aerogares, sem prejuízo das competências atribuídas por lei a outras entidade;
>
> . . . . . .
>
> *ab*) Colaborar com as autoridades judiciárias nos termos do disposto no Código de Processo Penal, procedendo à investigação dos crimes cuja competência lhe esteja especificamente atribuída por lei.»

Segundo o artigo 15.º, a ASAE detém poderes de autoridade e é órgão de polícia criminal (n.º 1); são autoridades de polícia criminal, nos termos e para os efeitos previstos no CPP, o inspetor-geral, os subinspetores-gerais, os diretores regionais, designados por inspectores-diretores, o diretor de serviço de planeamento e controlo operacional e os inspetores-chefes e os chefes de equipas multidisciplinares (n.º 2).

Do vasto elenco das suas atribuições, verifica-se que a ASAE tem uma vasta intervenção na fiscalização e prevenção do cumprimento da legislação reguladora do exercício das atividades económicas nos setores alimentar e não alimentar, incumbindo-lhe, nomeadamente, fiscalizar o cumprimento das obrigações legais dos agentes económicos e, bem assim, fiscalizar todos os locais onde se proceda a qualquer atividade industrial, comercial ou de prestação de serviços.

No âmbito das atribuições da ASAE, deverá incluir-se a fiscalização dos locais onde se proceda a quaisquer das atividades apontadas que envolvam objetos informáticos. Tenha-se em atenção a vertente económica associada aos programas de computador. A sua proteção jurídica visa, justamente, tutelar os direitos económicos dos seus autores.

Ora, no exercício destas atribuições, pode bem acontecer que se detetem suportes autónomos ou objetos contendo programas informáticos contrafeitos, no sentido de constituírem duplicação, não licenciada, de programas originais, deparando-se, consequentemente, com a veri-

ficação, em termos objetivos, do crime de reprodução ilegítima (não autorizada) de programa protegido.

Nesta situação de flagrante delito, a ASAE, tal como outras autoridades policiais e administrativas, tem competência para proceder à apreensão de tais suportes, conforme expressamente se dispõe no n.º 2 do artigo 201.º do Código do Direito de Autor e dos Direitos Conexos, oportunamente reproduzido ([80]).

Esta competência corresponde à que é prevista no n.º 4 do artigo 178.º, conjugado com a alínea *c*) do n.º 2 do artigo 249.º, ambos do CPP. De facto, no âmbito das *medidas cautelares e de polícia*, permite-se que os órgãos de polícia criminal procedam a apreensões no decurso de buscas e revistas ou quando haja urgência ou perigo de demora.

Como refere Paulo Dá Mesquita, estes atos cautelares e de polícia «dependem dos pressupostos de *necessidade e de urgência*, isto é, de um circunstancialismo que exige uma intervenção pronta do órgão de polícia criminal» ([81]).

Será exatamente com fundamento em motivo de urgência e de necessidade que a ASAE deverá proceder, no exercício das suas atribuições de fiscalização, nomeadamente de estabelecimentos comerciais ou de prestação de serviços, à imediata apreensão dos computadores ou de outros equipamentos informáticos em relação aos quais existam fundadas suspeitas de conterem instalados programas informáticos não licenciados, em violação dos direitos económicos dos *sus* autores.

Trata-se de uma medida cautelar cuja execução particularmente se impõe neste domínio em que, como se sabe, facilmente e de forma muito rápida, é possível a eliminação de *software* armazenado em computadores.

Nos termos do artigo 178.º, n.º 5, do CPP, as apreensões efetuadas ficam sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

4 — Importa, entretanto, consignar que, de acordo com o disposto na alínea *l*) do n.º 3 do artigo 7.º da Lei de Organização da Investigação Criminal (LOIC), aprovada pela Lei n.º 49/2008, de 27 de agosto, é da *competência reservada* da Polícia Judiciária a investigação dos crimes informáticos e praticados com recurso a tecnologia informática ([82]).

Tendo presentes as considerações tecidas a propósito da natureza e caracterização do crime de reprodução ilegítima de programa protegido e da conclusão a que se chegou, no sentido da sua inclusão no âmbito dos crimes informáticos, a sua investigação está reservada à Polícia Judiciária.

Neste enquadramento, impõe-se que se convoque o que se prescreve nos artigos 5.º, n.º 1, e 10.º, n.º 2, da LOIC.

Assim, nos termos do preceito primeiramente citado, o órgão de polícia criminal que tiver notícia do crime e não seja competente para a sua investigação apenas pode praticar os atos cautelares necessários e urgentes para assegurar os meios de prova.

O citado artigo 10.º, n.º 2, estabelece, por sua vez, a regra segundo a qual «os órgãos de polícia criminal devem comunicar à entidade competente, no mais curto prazo, que não pode exceder vinte e quatro horas, os factos de que tenham conhecimento relativos à preparação e execução de crimes para cuja investigação não sejam competentes, apenas podendo praticar, até à sua intervenção, os atos cautelares e urgentes para obstar à sua consumação e assegurar os meios de prova».

A seleção das normas legais aqui pertinentes, contidas na LOIC, não ficará completa sem a referência ao artigo 2.º do mesmo diploma, relativo à direção da investigação criminal. Proclamando-se o princípio segundo o qual a direção da investigação cabe à autoridade judiciária competente em cada fase do processo, preceitua o n.º 3 que os órgãos de polícia criminal, logo que tomem conhecimento de qualquer crime, comunicam o facto ao Ministério Público no mais curto prazo, sem prejuízo da prática dos atos cautelares necessários e urgentes para assegurar os meios de prova.

Da conjugação de todas estas regras, pode concluir-se, que, tendo qualquer órgão de polícia criminal conhecimento de factos tipificados como crimes cuja investigação se encontra legalmente reservada à Polícia Judiciária, deve comunicar-lhe e, bem assim, transmitir a notícia do crime ao Ministério Público.

O Ministério Público praticará, por si próprio, os atos de inquérito, assistido pelos órgãos de polícia criminal (artigo 267.º do CPP), ou delegará na Polícia Judiciária os atos, diligências ou investigações relativas ao inquérito (artigo 270, n.º 1, do CPP), tendo em conta a regra da «divisão legal das matérias de coadjuvação entre órgãos de polícia criminal» ([83]).

5 — Relativamente à questão de saber «em que moldes a ASAE deve atuar no âmbito da Lei n.º 109/2009, de 15 de setembro», dir-se-á, em síntese conclusiva:

A competência para a investigação dos crimes previstos na citada lei (Lei do Cibercrime), onde se inclui o crime de reprodução ilegítima de programa protegido, está reservada à Polícia Judiciária, pelo que somente a esta entidade poderá ser delegada a execução de atos de inquérito pelo Ministério Público;

A atuação da ASAE no âmbito de tais crimes está limitada à prática dos atos cautelares e urgentes, quer para obstar à sua consumação, quer para assegurar os meios de prova;

Assim, no decurso das suas ações de fiscalização de atividades económicas, deve proceder à apreensão dos suportes físicos autónomos de computadores (CD-ROMs, *pen disks*, disquetes, etc.) que contenham gravados programas informáticos objeto de contrafação, no sentido de constituírem reprodução não autorizada ou licenciada, bem como dos próprios computadores ou outros equipamentos informáticos em relação aos quais existam fundadas suspeitas de conterem *software* operativo sem a necessária licença dos legítimos detentores dos direitos de autor, comunicando o facto à Polícia Judiciária, em prazo não excedente a 24 horas, e ao Ministério Público para sua validação;

Por força da competência reservada da Polícia Judiciária para a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, nos quais se compreende o crime de reprodução não autorizada de programa protegido, está vedada à ASAE a pesquisa de dados informáticos armazenados em sistemas informáticos.

6 — Como nota final, cumpre referir que a análise aqui empreendida quanto ao âmbito de aplicação das disposições processuais previstas no capítulo III da lei do Cibercrime se circunscreveu aos crimes previstos neste diploma legal e, bem assim, aos crimes cometidos por meio de um sistema informático [alíneas *a*) e *b*) do n.º 1 do artigo 11.º], em cujas categorias incluímos o crime de reprodução ilegítima de programa protegido, referenciado no pedido de consulta.

Importa, entretanto, notar que a ASAE, no âmbito da investigação dos crimes cuja competência lhe esteja especificamente atribuída por lei, pode recorrer às disposições processuais previstas na lei do Cibercrime, com fundamento no disposto no seu artigo 11.º, n.º 1, alínea *c*), ou seja, em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico ([84]).

VII

Em face do exposto, formulam-se as seguintes conclusões:

1.ª O crime de reprodução ilegítima de programa protegido, previsto e punido pelo artigo 8.º da lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, assume a natureza de crime informático, como tal legalmente tipificado, e a sua prática envolve a utilização de um sistema informático, pelo que lhe são aplicáveis as disposições processuais contidas nos artigos 12.º a 17.º daquele diploma, conforme dispõe o seu artigo 11.º, n.º 1, alíneas *a*) e *b*), da mesma lei;

2.ª A competência para a investigação do crime de reprodução ilegítima de programa protegido, enquanto crime informático, está reservada à Polícia Judiciária, em conformidade com o disposto no artigo 7.º, n.º 3, alínea *l*), da Lei de Organização da Investigação Criminal, aprovada pela Lei n.º 49/2008, de 27 de agosto, podendo somente em tal entidade ser delegada a execução de atos de inquérito pelo Ministério Público;

3.ª A atuação da Autoridade de Segurança Alimentar e Económica (ASAE) no âmbito do crime referido na conclusão anterior, está limitada exclusivamente à prática dos atos cautelares e urgentes, quer para obstar à sua consumação, quer para assegurar os respetivos meios de prova;

4.ª No decurso das suas ações de fiscalização de atividades económicas, a ASAE deve, nos termos do disposto no artigo 201.º, n.º 2, do Código do Direito de Autor e dos Direitos Conexos, aprovado pelo Decreto-Lei n.º 63/85, de 14 de março, e nos artigos 178.º, n.º 4, e 249.º, n.os 1 e 2, alínea *c*), do Código de Processo Penal, proceder à apreensão dos suportes físicos exteriores de computador que contenham programas informáticos objeto de contrafação, bem como dos próprios computadores ou outros equipamentos informáticos em relação aos quais existam fundadas suspeitas de terem instalados programas não licenciados, comunicando o facto à Polícia Judiciária, em prazo não excedente a 24 horas, e ao Ministério Público para sua validação;

5.ª Por força da competência reservada da Polícia Judiciária para a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, nos quais se compreende o crime de reprodução não autorizada de programa protegido, está vedada à ASAE a pesquisa de dados informáticos armazenados em sistemas informáticos.

([1]) Formulado através do ofício GAJ — S/48081/SC, de 13 de abril de 2011. O parecer foi distribuído ao Conselho Consultivo da Procuradoria-Geral da República em 12 de maio de 2011, tendo sido redistribuído ao agora relator, por cessação de funções do relator inicial, em 16 de setembro de 2011.

([2]) Ofício GAJ — S/151225/11/SC, de 7 de dezembro de 2011.

([3]) Expressão utilizada por Cláudia Trabuco, "O direito de autor e as licenças de utilização sobre programas de computador — o contributo dos contratos para a compreensão do direito", *Themis — Revista da Faculdade de Direito da UNL*, Ano VIII — n.º 15 — 2008, pp. 139-169.

([4]) V. José Alberto Vieira, *A Proteção dos Programas de Computador pelo Direito de Autor*, Lex, Lisboa, 2005, pp. 12-16.

([5]) Aí se convoca a definição adotada nas Disposições Modelo da Organização Mundial da Propriedade Intelectual (OMPI) sobre a proteção dos suportes lógicos (Genebra, 1978), nos termos da qual, «programa de computador é um conjunto de instruções capaz, quando incorporado num meio legível por máquina, de levar uma máquina com capacidade de tratamento de informação a indicar ou executar uma função, tarefa ou resultado específico». Sobre o conceito, v. Vittorio Afferni, "Brevettabilità del software", *La tutela giuridica del software*, Giuffrè editore, p. 10, e Miguel Angel Davara Rodriguez, *Derecho Informático*, Aranzadi Editorial, p. 118. No direito comparado, conforme dá conta Alexandre Dias Pereira, é recorrente a consagração legal de programas de computador — *Informática, Direito de Autor e Propriedade Tecnodigital*, Stvdia Ivridica 55, *Boletim da Faculdade de Direito da Universidade de Coimbra*, Coimbra Editora, 2001, pp. 469-469, nota 856. No Brasil, a Lei n.º 9.609/98, de 19 de fevereiro de 1998, apresenta no seu artigo 1.º a seguinte noção de programa de computador: «é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados».

([6]) *Direito da Informática*, 2.ª edição refundida e atualizada, Almedina, 2006, p. 540.

([7]) "A proteção jurídica dos programas de computador", *Revista da Ordem dos Advogados*, ano 50, abril 1990, p. 72.

([8]) Acompanhou-se neste segmento expositivo José Alberto Vieira, *A Proteção dos Programas de Computador pelo Direito de Autor*, *cit.*, pp. 18-19, e Garcia Marques e Lourenço Martins, *ob. cit.*, p. 542.

([9]) Rui Saavedra, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores — Publicações Dom Quixote, Lisboa, 1998, p. 44.

([10]) *Idem*, *ibidem*.

([11]) Rui Saavedra, *A Proteção Jurídica do Software e a Internet*, *cit.*, p. 15.

([12]) *Ob. cit.*, p. 50.

([13]) "Software industry", *The Future of Intellectual Property in the Global Market of the Information Society*, Bruylant, Brussel-Bruxelles, 2003, p. 66.

([14]) I*dem*.

([15]) "Proteção de Programas de Computador na Comunidade Europeia — Em busca de um equilíbrio entre a proteção da Propriedade Intelectual e o Direito da Concorrência", *Direito e Justiça*, volume VII, 1993, p. 260. Sobre o tema da proteção jurídica do software, pode consultar-se também Miguel Angel Davara Rodriguez, *ob. cit.*, pp. 107 e segs.

([16]) Para uma descrição dos métodos e respetivas vantagens e inconvenientes, v. Rui Saavedra, *A Proteção Jurídica do Software e a Internet*, *cit.*, pp. 46-48, nota 73. O ideal, pondera este autor, «será ter, simultaneamente, uma eficaz proteção técnica e uma adequada proteção jurídica, ambas se complementando no desiderato último de tutelar os interesses em jogo dos criadores, produtores e distribuidores do *software*» (*ibidem*).

([17]) Rui Saavedra, *A Proteção Jurídica do Software e a Internet*, *cit.*, p. 73, que, de novo, se acompanha.

([18]) Alexandre Dias Pereira, "Software: sentido e limites da sua apropriação jurídica", *Temas de Direito da Informática e da Internet*, Ordem dos Advogados (Conselho Distrital do Porto), Coimbra Editora, 2004, pp. 74 e segs., que, neste passo se acompanha.

([19]) "Software: sentido e limites da sua apropriação jurídica", *Temas de Direito da Informática e da Internet*, *cit.*, p. 74.

([20]) Sobre os diversos modelos normativos para a proteção do *software*, v. José de Oliveira Ascensão, "A proteção jurídica dos programas de computador", *Revista da Ordem dos Advogados*, cit., 76-83, Rui Saavedra, ob. cit., pp. 70 e segs., Garcia Marques e Lourenço Martins, ob. cit., pp. 545-564, Alexandre Dias Pereira, "Software: sentido e limites da sua apropriação jurídica", *Temas de Direito da Informática e da Internet*, *cit.*, pp. 77 e segs., do mesmo autor, *Informática, Direito de Autor e Propriedade Tecnodigital*, *cit.*, pp. 461 e segs., José Alberto Vieira, ob. cit., pp. 21 e segs., António Vilhena de Carvalho, "Le droit d'auteur face aux nouvelles Technologies: le cas particulier du logiciel", Documentação e direito Comparado, *Boletim do Ministério da Justiça*, n.º 37/38, 1989, pp. 71 e segs., Adriana Camargo Rodrigues Casella, «Proteção do "software" pelo Direito de Autor», Revista da Faculdade de Direito, Universidade de São Paulo, volume 81, 1986 (Jan./Dez.), pp. 206-109, Vitorio Afferni, "Brevettabilità del software", *La tutela giuridica del software*, *cit.*, pp. 11-17, Antonio Piva e David d'Agostini, "La tutela giuridica dei programmi per elaboratore", disponível, na data de 03-01-2012, em www.mododigitale.net/Rivista/03/tutela_giuridica.pdf., e Peter Groves *et alii*, *Intellectual Property and the Internal Market of the European Community*, Graham & Trotman, 1993, pp. 82-88.

([21]) Aprovada, para ratificação, pelo Decreto n.º 52/91, de 30 de agosto.

([22]) Refira-se que, alguns anos antes, em 1964, o Copyright Office norte-americano aceitara um pedido de registo para proteção de um programa de computador.

([23]) *Jornal Oficial das Comunidades Europeias*, n.º L 122, de 17.5.91.

([24]) *Jornal Oficial da União Europeia*, n.º L 111, de 5.5.2009.

([25]) «TRIPS» corresponde à sigla de Trade Related Aspects of Intellectual Property.

([26]) Assim, relativamente aos ordenamentos que nos são mais próximos, refira-se que em Espanha a Ley de Propriedad Intelectual, aprovada pelo Real Decreto Legislativo 1/1996, de 12 de abril, estabelece que são objeto de propriedade intelectual todas as criações originais literárias, artísticas ou científicas expressas por qualquer meio ou suporte, tangível ou intangível, atualmente conhecido ou que se venha a inventar, compreendendo-se entre elas, nomeadamente, os programas de computador [artigo 10, alínea *i*)], dedicando aos «programas de ordenador» o título VII do Livro I (artigos 95 a 104). Em Itália, a fonte normativa da proteção dos programas de computador consta da Lei n.º 633, de 22 de abril, de 1941, com sucessivas alterações, sobre a «Protezione del diritto d'autore e di altri diritti connessi al suo esercizio» (secção VI — artigos 64-bis, 64-ter e 64-quater). Em França, a proteção do programa de computador (*logiciel*) está prevista no Code de la Propriété Intellectuelle (artigo 122-6).

([27]) Retificado pela Declaração de Retificação n.º 2-A/95, de 31 de janeiro, e alterado pelo Decreto-Lei n.º 334/97, de 27 de novembro.

([28]) Refira-se que os programas de computador, «enquanto tais», estão excluídos da patenteabilidade, conforme estabelece o artigo 52.º, n.º 1, alínea *d*), do Código da Propriedade Industrial.

([29]) "Software: sentido e limites da sua apropriação jurídica", *Temas de Direito da Informática e da Internet*, *cit.*, p. 92.

([30]) "Proteção jurídica e exploração negocial de programas de computador", *Boletim da Faculdade de Direito*, Universidade de Coimbra, volume comemorativo, Coimbra, 2003, p. 456.

([31]) *Ob. cit.*, p. 571.

([32]) *Ob. cit.*, p. 899.

([33]) Para uma análise do projeto do Decreto-Lei n.º 252/94, v. Pedro Cordeiro, «A lei portuguesa de "software"», *Revista da Ordem dos Advogados*, ano 54, vol. II, julho de 1994. Sobre a questão de saber se o programa de computador é obra literária, pode consultar-se José de Oliveira Ascensão, "A proteção jurídica dos programas de computador", *Revista da Ordem dos Advogados*, *cit.*, pp. 97 e segs.

([34]) Aprovado pelo Decreto-Lei n.º 63/85, de 14 de março, sucessivamente alterado, com republicação efetuada pela Lei n.º 16/2008, de 1 de abril.

([35]) Esta disposição está reproduzida no artigo 4.º, n.º 1, alínea *a*), da Diretiva 2009/24/CE.

([36]) *Ob. cit.*, p. 271.

([37]) A *Proteção dos Programas de Computador pelo Direito de Autor*, *cit.*, p.94.

([38]) Muito embora a Diretiva 91/250/CEE não a impusesse expressamente, a via penal de proteção dos programas de computador, o seu artigo 7.º, n.º 1, sobre as «medidas de proteção especiais», aponta para ela ao estabelecer que os Estados-membros tomarão medidas adequadas, nos termos das respetivas legislações nacionais, contra as pessoas que, nomeadamente, ponham em circulação uma cópia de um computador, conhecendo ou não podendo ignorar o seu caráter ilícito [alínea *a*)], ou estejam na posse, para fins comerciais, de uma cópia de um programa de computador, conhecendo ou não podendo ignorar o seu caráter ilícito [alínea *b*)]. Esta disposição é mantida no artigo 7.º da Diretiva 2009/24/CE. Nos termos do n.º 2 destes preceitos, qualquer cópia ilícita de um programa de computador pode ser confiscada nos termos da legislação do Estado-membro em questão.

([39]) *Direito Penal — Parte Especial*, Tomo I (Direito Penal Informático-Digital), Coimbra, 2009, p. 307.

([40]) *Ob. cit.*, pp. 307-308.

([41]) Aprovada pela Resolução da Assembleia da República n.º 88/2009, de 10 de julho de 2009, e ratificada pelo Decreto n.º 91/2009, de 15 de setembro.

([42]) "A nova lei do Cibercrime", estudo distribuído no Centro de Estudos Judiciários.

([43]) *Idem*.

([44]) A proteção legal dos programas informáticos é proclamada no artigo 1.º, n.º 2, do Decreto-Lei n.º 252/94, de 20 de outubro, desde que tenham «*caráter criativo*». Por seu lado, o artigo 14.º do mesmo diploma consagra expressamente a proteção penal para o programa de computador, determinando a aplicação do n.º 1 do artigo 9.º da Lei n.º 109/91, atualmente do artigo 8.º, n.º 1, da lei do Cibercrime.

([45]) S*upra IV.1*.

([46]) Cita-se José Alberto Vieira*, A Proteção dos Programas de Computador pelo Direito de Autor*, *cit.*, p. 94.

([47]) Comentário ao artigo 8.º da lei do Cibercrime, em *Comentário das Leis Penais Extravagantes*, Volume I, organização de Paulo Pinto de Albuquerque e José Branco, Universidade Católica Editora, 2010, p. 520.

([48]) V. Garcia Marques e Lourenço Martins, *ob. cit*., pp. 704-707, Lourenço Martins, "Criminalidade informática", *Direito da Sociedade de Informação*, Volume IV, Coimbra Editora, 2003, pp. 32-38, Rui Saavedra, *ob. cit*., pp. 289-292, José Alberto Vieira, *ob. cit.*, pp. 94-98, Pedro Dias Venâncio, lei *do Cibercrime Anotada e Comentada*, Coimbra Editora, 2011, pp. 75-76, e Alexandre Dias Pereira, *Informática, Direito de Autor e Propriedade Tecnodigital*, *cit.*, pp. 505-508.

([49]) Acórdãos do Tribunal da Relação do Porto de 23 de abril de 2003 (Processo 0240941), de 18 de junho de 2003, e de 16 de junho de 2004 (Processo 0342776), Acórdão do Tribunal da Relação de Coimbra de 5 de julho de 2006 (Processo 1159/06), Acórdão do Tribunal da Relação de Lisboa de 14 de junho de 2006 (Processo 3409/2006-3). Lê-se neste último aresto que a reprodução é «a fixação da obra num meio que permita a sua comunicação e a obtenção de cópias de toda ou de parte dela». Estes acórdãos encontram-se disponíveis em www.dgsi.pt.

([50]) *Ob. cit.*, p. 641.

([51]) *Idem*, *ibidem*. Sobre o conceito de criminalidade informática, v. também Benjamim Silva Rodrigues, *ob. cit.*, pp. 144 e segs, A. G. Lourenço Martins, "Criminalidade informática", *Direito da Sociedade de Informação*, Volume IV, Coimbra Editora, 2003, *cit.*, pp. 9 e segs., Pedro Dias Venâncio, lei *do Cibercrime Anotada e Comentada*, *cit.*, pp. 16-22, Lorenzo Picotti, "Biens juridiques protégés et techniques de formulation des incriminations en droit penal de l'informatique", *Revue Internationale de Droit Penal*, 77 [e] année, nouvelle série, 3 [e]/4 [e] trimestres, 2006, pp. 529 e segs., e Daniel Martin e Frédéric-Paul Martin, *Cybercrime: menaces, vulnérabilités et ripostes*, Presses Universitaires de France, 2001, pp. 13-16.

([52]) "Cibercrime", *Direito da Sociedade de Informação*, Volume IV, Coimbra Editora, 2003, p. 348.

([53]) *Ob. cit.*, p. 354.

([54]) Vem-se citando João Carlos Cruz Barbosa de Macedo, "Algumas considerações acerca dos crimes informáticos em Portugal", *Direito Penal Hoje — Novos desafios e novas respostas*, organização de Manuel da Costa Andrade e Rita Castanheira Neves, Coimbra Editora, 2009, p. 230.

([55]) Rita Coelho Santos, *O Tratamento Jurídico Penal da Transferência de Fundos Monetários através da Manipulação Ilícita dos Sistemas Informáticos*, Stvdia Ivridica 82, Coimbra Editora, 2005, pp. 32 e segs., citada pelo autor referido na nota anterior.

([56]) I*bidem*.

([57]) "O crime informático", *Revista de Investigação Criminal*, n.º 31, novembro 1989, p. 36.

([58]) "O crime informático", *Revista de Investigação Criminal*, n.º 32, fevereiro 1990, p. 43.

([59]) Cibercrime", *Direito da Sociedade de Informação*, Volume IV, *cit.*, pp. 354-355.

([60]) Um dos meios de tutela tem consistido, nomeadamente, no recurso ao procedimento cautelar cível, expressamente admitido no Código do Direito de Autor e dos Direitos Conexos — artigo 210.º-G. Ilustrando esta via, podem consultar-se as decisões judiciais coligidas por Manuel Lopes Rocha, em *Direito da Informática nos Tribunais Portugueses (1990-1998)*, Edições Centro Atlântico, 1999, pp. 53 e segs. V. também o acórdão do Tribunal da Relação de Coimbra de 9 de dezembro de 2008, também disponível em www.dgsi.pt.

([61]) A Lei n.º 32/2008 regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes.

([62]) Pedro Verdelho, "A nova lei do Cibercrime", *Estudo citado*.

([63]) *Ob. cit.*

([64]) *Diário da Assembleia da República* (*DAR*), 2.ª série A, n.º 120/X/4, de 23 de maio de 2009. A discussão na generalidade está documentada no *DAR*, 1.ª série, n.º 102/X/4, de 11 de julho de 2009. Sobre o âmbito desta lei e sobre a opção do legislador em não integrar as normas processuais que contempla no Código de Processo Penal, v. Paulo Dá Mesquita, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, pp. 95--101.

([65]) "A nova lei do Cibercrime", *Estudo citado.* Do mesmo autor, v. "Cibercrime", *Direito da Sociedade de Informação*, Volume IV, *cit.*, pp. 375-378. Sobre estas medidas processuais, pode consultar-se Benjamim Silva Rodrigues, *Da Prova Penal*, Tomo IV, 1.ª edição, Rei dos Livros, 2011, pp. 518-531, Pedro Dias Venâncio, *ob. cit.*, pp. 98 e segs., e Paulo Dá Mesquita, *Processo Penal, Prova e Sistema Judiciário*, *cit.*, pp. 112-113. V. também o Relatório justificativo da Convenção sobre Cibercrime, pontos 149 e segs.

([66]) P*rocesso Penal, Prova e Sistema Judiciário*, *cit.*, p. 115.

([67]) *Idem*, *Ibidem*.

([68]) Pedro Verdelho, "A nova lei do Cibercrime", *Estudo citado*.

([69]) Sobre o regime das buscas e das apreensões no processo penal, v. Germano Marques da Silva, *Curso de Processo Penal*, II, 3.ª edição, revista e atualizada, Editorial Verbo, 2002, pp. 213 e segs., Paulo Pinto de Albuquerque, *Comentário do Código de Processo Penal*, 3.ª edição atualizada, Universidade Católica Editora, 2009, pp. 174 e segs. e 667-668. No domínio do CPP anterior, cf. Manuel de Cavaleiro Ferreira, *Curso de Processo Penal*, vol. 1.º, Lisboa, 1986, págs. 233-236. O Conselho Consultivo também se tem pronunciado sobre este tema, como sucedeu, designadamente, no parecer n.º 127/2004, de 17 de março de 2005, e, mais recentemente, no parecer n.º 32/2010, ambos inéditos.

([70]) O conceito de sistema informático, para efeitos da lei do Cibercrime, consta da alínea *a*) do seu artigo 2.º Trata-se de um conceito amplo, nos termos do qual se considera *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, proteção e manutenção».

([71]) *Curso de Processo Penal*, I, 4.ª edição revista e atualizada, Editorial Verbo, 2000, p. 275.

([72]) *Ibidem*. Sobre esta figura, v. Maia Gonçalves, *Código de Processo Penal Anotado,* 16.ª edição — 2007, Almedina, Coimbra, 2007, p. 53.

([73]) D*ireção do Inquérito Penal e Garantia Judiciária*, Coimbra Editora, 2003, pp. 121-122.

([74]) *Ob. cit.*, p. 121 (nota 2).

([75]) M*odelos de Polícia e Investigação Criminal*, "O modelo português — a dependência funcional", intervenção no 1.º Congresso de Investigação Criminal, Porto, 16 e 17 de março de 2006, Edições Gailivro, julho de 2006, pp. 97 e segs. (p. 99). Sobre o sentido e alcance dos órgãos de polícia criminal, v., do mesmo Autor, *O Ministério Público e os Órgãos de Polícia Criminal no Novo Código de Processo Penal*, Porto, 1993, pp. 99-104.

([76]) *Ibidem*.

([77]) Acompanhou-se neste segmento expositivo o parecer n.º 28/2008, de 8 de maio de 2008 (*Diário da República,* 2.ª série, n.º 155, de 12 de agosto de 2008).

([78]) Como a Direção-Geral do Controlo e Fiscalização da Qualidade Alimentar, a Inspeção-Geral das Atividades Económicas e a Agência Portuguesa de Segurança Alimentar, cujas competências transitaram para a ASAE.

([79]) O Tribunal Constitucional, pelo acórdão n.º 84/2010, de 3 de março, não julgou inconstitucionais as normas da alínea *aa*) do n.º 2 do artigo 3.º do Decreto-Lei n.º 274/2007, de 30 de julho, enquanto atribui competências à ASAE para desenvolver ações de natureza preventiva e repressiva em matéria de jogo ilícito, e do artigo 15.º deste decreto-lei, na parte em que confere poder de órgãos e autoridade de polícia criminal à ASAE, em conjugação com a atribuição de competências para prevenir certos crimes; no mesmo sentido, em relação às normas dos artigos 3.º, n.º 2, alínea *h*), e 15.º, v. o acórdão n.º 232/2010, de 15 de junho. Estes acórdãos estão disponíveis em www.tribunalconstitucional.pt.

([80]) Redação da Lei n.º 16/2008, de 1 de abril.

([81]) "Repressão criminal e iniciativa própria dos órgãos de polícia criminal", *Revista do Ministério Público*, ano 25.º, abril-junho 2004, n.º 98, p. 11.

([82]) Sem prejuízo de, nos termos do artigo 8.º, n.º 1, da LOIC, a sua investigação, na fase de inquérito, ser deferida pelo Procurador-Geral da República a outro órgão de polícia criminal, desde que tal se afigure, em concreto, mais adequado ao bom andamento da investigação e quando ocorra qualquer uma das circunstâncias enumeradas nas suas alíneas.

([83]) Sobre este ponto, v. Paulo Dá Mesquita, *Processo Penal, Prova e Sistema Judiciário*, *cit.*, pp. 393-394.

([84]) Sobre este tópico e quanto à articulação da norma citada com o artigo 189.º, n.º 1, do CPP, v. Paulo Dá Mesquita, *Processo Penal, Prova e Sistema Judiciário*, *cit.*, pp. 95-111.

Este parecer foi votado na sessão do Conselho Consultivo da Procuradoria-Geral da República, de 26 de janeiro de 2012.

Isabel Francisca Repsina Aleluia São Marcos — Manuel Pereira Augusto de Matos (relator) — Fernando Bento — António Leones Dantas — Maria Manuela Flores Ferreira — Paulo Joaquim da Mota Osório Dá Mesquita — Alexandra Ludomila Ribeiro Fernandes Leitão — Maria de Fátima da Graça Carvalho.

Por despacho de 14 de maio de 2012, o Procurador-Geral da República determinou que a doutrina deste parecer seja seguida e sustentada pelos Magistrados do Ministério Público (artigos 12.º n.º 2, alínea *b*), e 42.º, n.º 1, do Estatuto do Ministério Público).

Está conforme.

24 de maio de 2012. — O Secretário da Procuradoria-Geral da República, *Carlos José de Sousa Mendes*.

206133096