ARTÍCULOS

USO DE *MALWARE* EM INVESTIGAÇÃO CRIMINAL

Daniel Bento Alves
*Advogado**

Uso de *malware* em investigação criminal

No contexto da actual sociedade alicerçada em tecnologias de informação e da acelerada mutação do sistema processual penal garantístico para um sistema que procura, essencialmente, a eficácia na perseguição penal, surge, por influência, essencialmente, Estado--Unidense, a possibilidade de as autoridades de investigação criminal recorrerem a um método oculto de investigação criminal - malware - para monitorização e realização de buscas informáticas online (em tempo real) nos sistemas informáticos dos visados. Este artigo visa responder à questão de saber se o sistema processual penal Português já prevê a possibilidade de se recorrer a este método oculto de investigação criminal.

Use of *malware* in criminal investigation

In the context of the current society based on information technology services and the accelerated mutation from a protectionist criminal procedure system to a system that aims, essentially, to promote the effectiveness of the criminal investigation, it arises the possibility – inspired in the US system – of the criminal investigation authorities use an undercover investigation method – malware – to monitor and perform online searches (in real time) in the computerized systems of the suspects. This article intends to answer to the question if the Portuguese criminal procedure system already foresees the possibility of using this undercover investigation method.

Palavras-chave
Acções encobertas, Malware, Métodos ocultos de investigação, Processo penal.

Key words
Undercover actions, Malware, Undercover investigation methods, Criminal procedure.

Fecha de recepción: 15-9-2017

Fecha de aceptación: 31-10-2017

INTRODUÇÃO

Actualmente, a *vox populi* em Portugal é a de que o sistema processual penal Português é, essencialmente, garantístico, isto é, protege os arguidos, subalternizando a eficácia na perseguição penal. Suportadas nesta ideia generalizada, são várias as vozes que têm vindo a terreiro sufragar a adopção de institutos controversos como, por exemplo, a delação premiada ou o crime de enriquecimento ilícito.

Contudo, a verdade é que, quando analisados e concatenados os vários regimes especiais de cariz processual penal com o actual regime geral - Código de Processo Penal (CPP) -, coloca-se a questão de saber se o sistema processual penal Português ainda hoje é suficientemente garantístico ou, pelo menos, compatível e aceitável à luz da Constituição da República Portuguesa.

De facto, no contexto de uma sociedade alicerçada em tecnologias de informação, a criminalidade assumiu novas formas, tornando-se cada vez mais complexa, sofisticada e, sobretudo, munida de uma rápida capacidade de adaptação, o que exige do legislador penal um constante esforço de criação de meios especiais e excepcionais de combate ao crime.

A resposta do legislador penal a esta complexa realidade criminal – através da criação de diversos regimes especiais e excepcionais – leva alguns Autores a concluir, inclusivamente, que o paradigma do sistema processual penal garantístico findou e que se está perante uma nova fase de busca (a todo o custo) pela eficácia no combate ao crime.

Nas palavras de Costa Andrade: "*…as novações legislativas a que nos vimos reportando convergem*

* Del Área de Derecho Público, Procesal y Arbitraje de Uría Menéndez Proença de Carvalho (Lisboa).

todas no mesmo sentido final: redução e neutralização de garantias de defesa; multiplicação, em número e potencial de lesividade e devassa, dos meios institucionalizados de intromissão nos direitos fundamentais; deslocação das linhas de equilíbrio normativo do lado da liberdade, da autonomia e da dignidade, para o lado da segurança; do lado da justiça e da «superioridade ética do Estado» (Eb. Schimdt), *para o lado da eficácia e da Funktionstütigkeit der Strafrechtspflege; do arguido para a ordem, a reafirmação da validade das normas e, aqui e ali, os interesses da vítima*" ("Métodos ocultos de investigação (Plädoyer para uma teoria geral)", *in Que futuro para o Direito Processual Penal?*, 2009, Coimbra Editora, página 528).

É justamente neste contexto de (aparente) mutação do sistema processual penal "*garantístico*" para um sistema de "*combate ao crime*" que surge a discussão sobre a possibilidade de utilização de meios ocultos ou encobertos de investigação criminal em ambiente digital, mais especificamente o *malware*.

O presente artigo visa, justamente, fazer uma incursão sobre a questão de saber se a figura do *malware* – enquanto meio oculto ou encoberto de investigação criminal – já se encontra consagrada no sistema processual penal Português.

O QUE É O *MALWARE*?

Do ponto de vista informático, o termo *malware* resulta da contracção do adjectivo *malicious* (malicioso) e do substantivo *software* (programa informático) e pode ser definido, nas palavras de David Silva Ramalho, como "*um programa simples ou auto-replicativo que directamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade do sistema ou para assegurar que o utilizador seja incriminado por um crime informático*" ("O uso de malware como meio de obtenção de prova", *in Revista de Concorrência e Regulação n.º 16*, 2013, páginas 201 e 202).

Ou seja, o *malware* constitui um programa instalado sub-repticiamente num sistema informático sem o conhecimento do respectivo proprietário / utilizador com o objectivo, entre outros, de monitorizar, em tempo real, a respectiva actividade, isto é, de realizar *buscas online*[1].

A pedra de toque do *malware* é que o mesmo é instalado sub-repticiamente, através de *hacking*, no sistema informático do sujeito alvo (isto é, sem o seu conhecimento) através de diversos meios: *(i)* infecção via suporte físico removível; *(ii)* infecção via *browser*; e *(iii)* infecção via *download* voluntário.

Existem diversos tipos de *malware*, desde os célebres cavalos de Tróia ("*Trojan horses*") até às *logic bombs*, *spyware*, *rootkits*, *worms*, etc. Por exemplo, os mais vulgares "cavalos de Tróia" são instalados no sistema informático "alvo" da mesma maneira que os Troianos abriram as portas aos Gregos para receberem o cavalo de madeira, isto é, através de um comportamento voluntário do utilizador/proprietário do sistema informático (por exemplo, através do *download* de um anexo de uma mensagem de correio electrónico, etc.).

Portanto, a capacidade do *malware* para obter informação / documentação – de forma oculta – é avassaladora. Aliás, recentemente, têm vindo a lume diversos casos que, alegadamente, terão resultado de *hacking* de particulares, como, por exemplo, os *Panama Papers* ou *Football Leaks*[2]. Naturalmente que estes casos – (alegado) *hacking* de particulares – resultam de alegada actividade criminalmente relevante, que, como tal, torna impossível a utilização da documentação / informação apreendida num hipotético processo-crime.

Assim, o uso de *malware* no contexto de uma investigação criminal consistiria, em traços gerais, na instalação sub-reptícia de um *software* informático em qualquer sistema ou suporte informático (*v.g.* computador, *tablet*, *smart phone*, etc.) de um visado com o objectivo de as autoridades de investigação criminal monitorizarem, em tempo real, a actividade informática daquele através da vigilância permanente desse mesmo sistema ou suporte informático e, assim, obter provas para a investigação criminal que se encontra em curso[3].

Como é evidente, o uso de *malware* é particularmente intrusivo, na medida em que permite ter

1 Ao longo deste artigo, as expressões "*uso de malware*" e "*buscas online*" serão utilizadas, indistintamente, com o mesmo significado. Assim sendo, a expressão "*busca online*" não se resumirá à pesquisa de informação/documentação num determinado sistema informático, mas à monitorização, em tempo real e de forma sub-reptícia, de um determinado sistema informático.

2 Daí que, hodiernamente, as empresas invistam recursos substanciais em programas de segurança informática para evitar fenómenos de *hacking*.

3 É hoje conhecido que o FBI infecta computadores de suspeitos/visados com *malware* no âmbito das respectivas investigações criminais (https://www.itnews.com.au/news/fbi-used-malware-in-criminal-investigation-390688).

acesso, em tempo real, a toda a actividade que um determinado proprietário / utilizador executar através de um determinado sistema informático.

A questão que se coloca é a de saber se as autoridades de investigação criminal Portuguesas têm, ou não, a faculdade de recorrer ao *malware* para obtenção de prova. Isto é: à semelhança de um *hacker*, pode também o Estado aceder – de forma encoberta – ao computador (ou, por exemplo, a um *smart phone*) de um suspeito e monitorizar, em tempo real, a actividade que mesmo suspeito desenvolve nesse computador?

Como pano de fundo de análise desta questão, importa ter em consideração os princípios subjacentes aos meios de obtenção de prova, assim como o regime das acções encobertas e, finalmente, as disposições processuais introduzidas pela Lei do Cibercrime, aprovada pela Lei. n.º 109/2009 ("**Lei do Cibercrime**"). Comecemos pelo primeiro ponto.

PRINCÍPIOS SUBJACENTES AOS MEIOS DE OBTENÇÃO DE PROVA

Os meios de obtenção de prova são, como ensina Germano Marques da Silva, "*instrumentos de que se servem as autoridades judiciárias para investigar e recolher meios de prova; não são instrumentos de demonstração do thema probandi, são instrumentos para recolher no processo esses instrumentos*". Como é óbvio, os "*meios de obtenção de prova*" não se confundem com os "*meios de prova*" propriamente ditos. De facto, os meios de prova constituem "*os elementos de que o julgador se pode servir para formar a sua convicção sobre um facto*" (Curso de Processo Penal, Vol. II, Editorial Verbo, 1999, página 189).

O artigo 125.º do CPP dispõe, sob a epígrafe "*Legalidade da Prova*", que "*são admissíveis as provas que não forem proibidas por lei*". Concomitantemente, o artigo 126.º do CPP prevê, sob a epígrafe "*Métodos proibidos de prova*", um conjunto de provas proibidas. Numa leitura apressada, resultaria da conjugação destas duas normas que, em princípio, seriam admitidos quaisquer meios de prova e, concomitantemente, quaisquer meios de obtenção de prova, desde que os mesmos não se encontrassem legalmente proibidos.

Contudo, esta conclusão seria, naturalmente, precipitada. De facto, no sistema processual penal, vigora o princípio da legalidade da prova. Por conseguinte, e em princípio, a prova deve ser feita de acordo com os termos previstos na lei. Como explica David Silva Ramalho: "*…no processo penal vigora o princípio da legalidade e não da atipicidade da prova, de onde decorre que a prova deve ser feita, não apenas nas margens da não proibição, mas sim nos termos da lei, excepto quando esta se revele insuficiente e não haja obstáculo ao recurso a meios de prova ou de obtenção de prova atípicos*" (Métodos Ocultos de Investigação Criminal em Ambiente Digital, 2017, Almedina, página 214).

Nas situações em que um concreto meio de obtenção de prova não se encontre regulado na lei, isto é, seja atípico – e não seja automaticamente excluído por força do n.º 8 do artigo 32.º da Constituição da República Portuguesa ou do artigo 126.º do CPP – há que verificar se o mesmo não constitui uma restrição a direitos fundamentais. Caso constitua efectivamente uma restrição a direitos fundamentais não prevista em lei, tal meio de obtenção de prova não é admissível.

De facto, ao abrigo do disposto no artigo 18.º da Constituição da República Portuguesa, qualquer restrição aos direitos fundamentais – como, por exemplo, um meio oculto de obtenção de prova – só é constitucionalmente legítima se (i) for autorizada na Constituição da República Portuguesa; (ii) estiver suficientemente sustentada em lei da Assembleia da República ou em decreto-lei autorizado; (iii) visar a salvaguarda de outro direito ou interesse constitucionalmente protegido; (iv) for necessária a essa salvaguarda, adequada para o efeito e proporcional a esse objectivo; (v) tiver carácter geral e abstracto, não tiver efeito retroactivo e não diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais.

Nas palavras de Paulo Pinto de Albuquerque: "*Quando o meio de obtenção de prova implicar um elevado grau de intrusão na privacidade do suspeito (ou um potencial aditivo de perigo inerente ao ataque aos direitos fundamentais (…), ele deve ser previsto por uma lei expressa (…)*"(Comentário do Código de Processo Penal, 2011, Universidade Católica Editora, página 332).

Além deste limite formal – relacionado com o princípio da reserva de lei –, há limites materiais intrínsecos aos meios atípicos de obtenção de prova, em particular os seguintes: (i) não são admissíveis meios de obtenção de prova que impliquem uma "*vigilância total*"; e (ii) não são admissíveis meios de obtenção de prova discriminatórios. Como explica Paulo Pinto de Albuquerque: "*Além destes limites formais, há limites materiais intrínsecos*

dos meios atípicos de obtenção de prova. O primeiro desses limites é o da inadmissibilidade da utilização, isolada ou coordenada, dos meios de obtenção de prova que permita uma vigilância total, com a qual possa ser construído um perfil completo da personalidade do arguido (…). Também não são admissíveis os meios de obtenção de prova discriminatórios, como por exemplo uma base de dados relativa exclusivamente a estrangeiros (…), nem os meios de obtenção de prova desproporcionais" (Comentário do Código de Processo Penal, 2011, Universidade Católica Editora, páginas 332 e 333).

Passemos, agora, a uma brevíssima análise do regime das acções encobertas previsto no ordenamento jurídico Português, onde a utilização de *malware* em investigações criminais - enquanto meio encoberto de investigação - se enquadra.

ACÇÕES ENCOBERTAS – REGIME GERAL

As acções encobertas consistem, naturalmente, num meio de obtenção de prova, mais especificamente em acções levadas a cabo por agentes de investigação (da polícia ou sob o seu controlo) - considerados agentes encobertos ou infiltrados -, com ocultação da respectiva qualidade e identidade, com o objectivo de recolher provas ou informações.

Para melhor delimitação da figura do *agente encoberto* é conveniente confrontá-lo com a figura do *agente provocador*. O *agente provocador* será aquele que instiga outrem à prática de um crime, isto é, tem um papel decisivo na formação da vontade criminal. Por contraposição, o *agente encoberto ou infiltrado* será aquele que não determina outrem à prática do crime, mantendo-se à margem da formação de vontade de cometer o ilícito criminal.

O recurso às acções encobertas para efeitos de uma investigação criminal coloca em causa diversos princípios fundamentais de um Estado de Direito Democrático, em particular o direito do arguido ao silêncio e a não se auto-incriminar, assim como o princípio da transparência e de lealdade da entidade que investiga, razão pela qual é excepcional.

De facto, o carácter dissimulado do agente encoberto constitui, evidentemente, uma actuação desleal por parte da entidade que investiga. Como explica Germano Marques da Silva: "*…a lealdade não é uma noção jurídica autónoma, é sobretudo de natureza essencialmente moral, e traduz uma maneira de ser da investigação e obtenção das provas em conformidade com o respeito dos direitos da pessoa e a dignidade da justiça. A actuação desleal como meio de investigação é sempre reprovável moralmente, embora nem sempre sancionada juridicamente*" ("Bufos, infiltrados, provocadores e arrependidos", *in Direito e Justiça*, Universidade Católica Editora, 1994, página 30).

Todavia, a verdade é que, actualmente, o recurso às acções encobertas é uma realidade incontornável na condução de uma investigação criminal. O n.º 8 do artigo 32.º da Constituição da República Portuguesa não exclui liminarmente a admissibilidade do recurso às acções encobertas. Contudo, para passarem o escrutínio constitucional, as acções encobertas têm de ser excepcionais, proporcionais e estar sujeitas a um apertado conjunto de pressupostos de admissibilidade e de controlo da sua utilização. Como explica Sandra Pereira: "*julgamos que não se deve excluir imediatamente a utilização do agente infiltrado. No entanto, por constituir um meio oculto de obtenção de prova e por respeito aos princípios constitucionalmente protegidos da dignidade humana e da integridade moral dos cidadãos, há que impor restrições a este método de investigação e às provas daí decorrentes*" ("A Recolha de Prova por Agentes Infiltrados", *in Prova Criminal e Direito de Defesa*, Almedina, 2015, página 146).

Além disso, e enquanto meio de obtenção de prova restritivo de direitos fundamentais, a possibilidade de se recorrer às acções encobertas encontra-se, naturalmente, sujeita à reserva de lei. Como explica Eduardo Maia Costa: "*A excepcionalidade dos meios de investigação ocultos, e particularmente, das acções encobertas, implica um regime jurídico com características específicas, para salvaguarda dos direitos fundamentais, em que avulta, desde logo, a exigência de uma reserva de lei. A significar que este meio de obtenção de prova só tem legitimidade na estrita medida em que goza de previsão legal, estando consequentemente vedado o recurso à analogia*" ("Acções Encobertas (Alguns problemas, algumas sugestões)", *in Estudos em Memória do Conselheiro Artur Maurício*, Coimbra Editora, 2014, página 361).

Ciente deste princípio da reserva de lei, o legislador penal veio consagrar a possibilidade de recurso às acções encobertas na Lei n.º 101/2001, de 25 de Agosto ("**Lei n.º 101/2001**").

O n.º 2 do artigo 1.º da Lei n.º 101/2001 define acções encobertas como "*aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade*". Ou

Ou seja, as acções encobertas podem ser levadas a cabo não só por "*funcionários de investigação criminal*" (isto é, funcionários da PJ, PSP e SEF), mas também por "*terceiros actuando sob o controlo da Polícia Judiciária*"[4] (isto é, particulares sem qualquer vínculo de fidelidade ao Estado, mas "*contratados*" pela Polícia Judiciária).

De acordo com a Lei n.º 101/2001, apenas é admissível recorrer a acções encobertas no âmbito da "*prevenção e repressão*" dos crimes taxativamente previstos no catálogo previsto no artigo 2.º. Assim, e como explica Eduardo Maia Costa, "*é no âmbito da investigação desses crimes, e apenas desses, que as acções encobertas podem ser praticadas*" ("Acções Encobertas (Alguns problemas, algumas sugestões)", *in Estudos em Memória do Conselheiro Artur Maurício*, Coimbra Editora, 2014, página 361).

Todavia, o catálogo previsto na Lei n.º 101/2001 é de tal modo amplo que o legislador penal parece pretender transformar um meio de obtenção de prova excepcional num meio de prova vulgar e banal.

Note-se ainda que a possibilidade de recurso às acções encobertas pode ocorrer quer no âmbito da repressão criminal, quer no âmbito da prevenção criminal dos crimes identificados no artigo 2.º da Lei n.º 101/2001. Deste modo, e mesmo que não se encontre em curso uma investigação (inquérito), é possível recorrer-se ao instituto das acções encobertas para fins estritamente de prevenção criminal.

Todavia, para que o recurso às acções encobertas seja admissível, é ainda necessário que, no caso concreto, essas acções sejam adequadas à descoberta da verdade material (isto é, que sejam profícuas num juízo de prognose), proporcionais (isto é, que sejam adequadas à gravidade do crime investigado) e estritamente necessárias, ou seja, que apenas sejam utilizadas caso não hajam outros meios menos invasivos igualmente idóneos para prosseguir a investigação eficazmente.

Para além da reserva de lei, a possibilidade de se recorrer às acções encobertas encontra-se também sujeita ao princípio da reserva de juiz. Como explica Eduardo Maia Costa: "*à reserva de lei acresce um requisito (e garantia fundamental): a reserva de juiz. A intervenção do juiz tem obviamente uma função garantística do maior relevo: a de assegurar a tutela preventiva dos direitos fundamentais*" ("Acções Encobertas (Alguns problemas, algumas sugestões)", *in Estudos em Memória do Conselheiro Artur Maurício*, Coimbra Editora, 2014, página 363).

Assim, o artigo 3.º da Lei n.º 101/2001 distingue consoante se trate de um inquérito em curso ou de estrita prevenção criminal. Caso esteja um inquérito em curso, o recurso às acções encobertas depende de prévia autorização do competente magistrado do Ministério Público, cabendo ao juiz de instrução a subsequente validação dessa autorização. Se o recurso às acções encobertas ocorrer no âmbito estrito da prevenção criminal, é competente para a autorização o juiz de instrução criminal.

A doutrina e jurisprudência têm entendido que a intervenção do juiz não se limita ao binómio aprovação / rejeição do recurso às acções encobertas, mas, nas palavras de Eduardo Maia Costa, abrange necessariamente "*a duração da acção, já que esta não pode ser indeterminada (pelo menos, não pode exceder o prazo do inquérito, podendo ser inferior), e também a eventual prorrogação e as modificações que ocorram no seu decurso, e ainda a delimitação dos actos a praticar pelo agente encoberto*" ("Acções Encobertas (Alguns problemas, algumas sugestões)", *in Estudos em Memória do Conselheiro Artur Maurício*, Coimbra Editora, 2014, página 363).

Após a execução da acção encoberta, a Polícia Judiciária "*fará o relato da intervenção do agente encoberto à autoridade judiciária competente no prazo máximo de quarenta e oito horas após o termo daquela*" (cfr. n.º 6 do artigo 3.º da Lei 101/2001). O relato da acção encoberta não constitui, em si mesmo, um meio de prova, servindo apenas para fiscalização da actividade do agente por parte das autoridades judiciárias. No entanto, o agente encoberto pode ter recolhido meios de prova no âmbito da acção encoberta ou mesmo intervir como testemunha nos autos, ao abrigo do disposto no n.º 4 do artigo 4.º da Lei 101/2001.

Naturalmente que as provas recolhidas no âmbito de uma acção encoberta que seja considerada ilegal serão sempre tidas como nulas e não poderão ser utilizadas no processo, nos termos e para os efeitos do disposto no n.º 2 do artigo 126.º do CPP.

Vejamos agora, em traços gerais, as disposições processuais introduzidas pelo legislador penal através da Lei do Cibercrime.

4 Os designados "*homens de confiança*".

AS NORMAS PROCESSUAIS - INCLUINDO O RECURSO ÀS ACÇÕES ENCOBERTAS – INSTITUÍDAS PELA LEI DO CIBERCRIME

Por força da Decisão Quadro n.º 2005/222/JAI, de 16 de Março de 2005, e da Convenção do Conselho da Europa sobre Cibercrime, CTS n.º 185, o legislador instituiu a Lei do Cibercrime.

No Capítulo III, a Lei do Cibercrime institui um conjunto de disposições processuais que visou suprir uma carência do ordenamento jurídico nacional relativamente à recolha de prova electrónica. Ao abrigo do disposto no artigo 11.º da Lei do Cibercrime, as disposições processuais da Lei do Cibercrime aplicam-se não apenas aos crimes informáticos *stricto sensu*, mas também aos crimes cometidos por meio de um sistema informático e aos crimes em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

Ou seja, como explica Paulo Dá Mesquita, "*as regras de direito probatório previstas neste diploma* [Lei do Cibercrime] *não são assim meras normas processuais sobre cibercrimes ou sequer apenas relativas a crimes praticados em sistemas informáticos, mas correspondem a um regime consideravelmente mais abrangente sobre prova electrónica em processo penal na lei sobre cibercriminalidade e não no Código de Processo Penal*" ("Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português - o Código e a Lei do Cibercrime", *in Processo Penal, Prova e Sistema Judiciário*, Wolters Kluwer/Coimbra Editora, 2010, página 98).

Portanto, a Lei do Cibercrime instituiu, nas palavras de João Conde Correia, "*um verdadeiro sistema processual de prova digital*" ("Prova digital: as leis que temos e a lei que devíamos ter", *in Revista do Ministério Público*, n.º 139, Setembro 2014, página 35).

Em primeiro lugar, o artigo 12.º da Lei do Cibercrime criou a possibilidade de as autoridades responsáveis por uma investigação criminal ordenarem a quem tenha disponibilidade ou controlo sobre dados informáticos específicos, designadamente a fornecedores de serviços, que preservem esses mesmos dados. Trata-se, no fundo, de uma medida cautelar de conservação de prova não intrusiva que apenas tem por finalidade a conservação de dados informáticos nas situações em que "*haja receio*" de que os mesmos se possam perder, alterar ou deixar de estar disponíveis.

Em segundo lugar, o artigo 13.º da Lei do Cibercrime instituiu o mecanismo da "*revelação expedita de dados de tráfego*". Esta norma obriga os fornecedores de serviços que devem assegurar a preservação dos dados informáticos nos termos do já aludido artigo 12.º da Lei do Cibercrime, a informarem as autoridades judiciárias ou os órgãos de polícia criminal competentes, logo que o souberem, quais são os "*outros fornecedores de serviço através dos quais*" uma determinada comunicação "*tenha sido efectuada*".

O objectivo desta norma é o de garantir que as autoridades judiciárias ou os órgãos de polícia criminal responsáveis pela investigação criminal tomem conhecimento - com a maior celeridade possível – de qual o percurso informático de uma determinada comunicação informática, isto é, quais os fornecedores de serviços que intervieram em todo o processo de envio e recepção de uma determinada comunicação.

Como explica Pedro Verdelho: "*Portanto, a obtenção com eficácia deste percurso* [da comunicação] *está dependente da expedita prestação de informação, a quem investiga, de cada um dos servidores, sobre o servidor que se segue no caminho da comunicação. É por esta razão que, na obtenção de informação sobre o percurso de uma comunicação, tendo em vista por exemplo determinar a sua origem, ou o seu destino, se torna imprescindível obter de forma expedita a revelação de dados de tráfego parcelares. Ao encontro desta realidade, a Lei prevê no art. 13.º a revelação expedita de dados de tráfego, a qual deverá ser providenciada pelos fornecedores de serviço às autoridades judiciárias ou aos órgãos de polícia criminal*" ("Lei do Cibercrime", *in Scientia Juridica*, Tomo LVIII, n.º 320, 2009, páginas 737 e 738).

Em terceiro lugar, o artigo 14.º da Lei do Cibercrime prevê a possibilidade de a autoridade judiciária competente ordenar a quem tenha disponibilidade ou controlo sobre determinados dados informáticos que os "*comunique ao processo ou que permita o acesso aos mesmos*", sob pena de punição por desobediência. No fundo, este artigo 14.º da Lei do Cibercrime permite que, por exemplo, a autoridade judiciária ordene a um fornecedor de serviço que comunique determinados dados informáticos à investigação.

Naturalmente que a injunção prevista neste artigo 14.º da Lei do Cibercrime não pode ser dirigida a suspeitos ou arguidos, sob pena de violação do direito à não auto incriminação. Nas palavras de Pedro Verdelho: "*Como se disse, é portanto claro no texto da lei que a injunção* [do artigo 14.º] *não pode ser dirigida a suspeitos ou arguidos. Se não fosse assim, a disposição colidiria com o direito à não auto incrimi-*

nação" ("Lei do Cibercrime", *in Scientia Juridica*, Tomo LVIII, n.º 320, 2009, página 739).

Com particular relevância para o exercício da advocacia, é igualmente cristalino que a injunção prevista neste artigo 14.º da Lei do Cibercrime não se aplica a sistema informáticos "*utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista*" (cfr. n.º 7 do artigo 14.º da Lei do Cibercrime).

Em quarto lugar, nos artigos 15.º a 17.º da Lei do Cibercrime prevê-se a pesquisa e apreensão de dados informáticos, assim como a apreensão de correio electrónico.

De facto, o artigo 15.º da Lei do Cibercrime prevê especificamente a possibilidade de se efectuarem "*buscas informáticas*" com o objectivo de se "*obter dados informáticos específicos e determinados, armazenados num determinado sistema informático*". Ou seja, o artigo 15.º da Lei do Cibercrime mais não é do que a adaptação das buscas previstas no CPP ao ambiente digital (cfr. n.º 6 do artigo 15.º da Lei do Cibercrime).

Concomitantemente, o artigo 16.º da Lei do Cibercrime regula a apreensão dos dados ou documentos informáticos que forem encontrados no decurso de uma pesquisa informática (ao abrigo do artigo 15.º da Lei do Cibercrime) e que tenham em vista a "*descoberta da verdade*".

Já o artigo 17.º da Lei do Cibercrime prevê as condições para a apreensão de correio electrónico ou registos de comunicações de natureza semelhante encontrados no decurso de uma pesquisa informática prevista no artigo 15.º da Lei do Cibercrime.

Em quinto lugar, o artigo 18.º da Lei do Cibercrime constitui uma adaptação do regime de intercepção de comunicações previsto no CPP ao ambiente digital. Nas palavras de Pedro Verdelho: "*O propósito do art. 18.º da Lei do Cibercrime é precisamente enquadrar legalmente a realização dessas intercepções de comunicações quando estiverem em investigação crimes considerados neste diploma*" ("Lei do Cibercrime", *in Scientia Juridica*, Tomo LVIII, n.º 320, 2009, páginas 746 e 747).

Em sexto lugar, o artigo 19.º da Lei do Cibercrime prevê a possibilidade de recurso a acções encobertas no ambiente digital[5].

Para este efeito, e através do n.º 1 do artigo 19.º da Lei do Cibercrime, o legislador penal aumentou significativamente o catálogo de crimes previsto no acima referido artigo 2.º da Lei n.º 101/2001, o que, como explica Paulo Dá Mesquita, "*no plano jurídico-constitucional, transgride, claramente, a linha do admissível, ao prever uma medida de carácter muito excepcional para um leque muito amplo de crimes*" ("Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português - o Código e a Lei do Cibercrime", *in Processo Penal, Prova e Sistema Judiciário*, Wolters Kluwer/Coimbra Editora, 2010, página 98).

Acresce que o n.º 2 do artigo 19.º da Lei do Cibercrime contém uma disposição formulada em termos vagos e, aparentemente, inócuos quando interpretada no sentido de visar tão-somente facultar ao agente encoberto a possibilidade de recorrer a quaisquer outros meios e dispositivos informáticos previstos na lei processual penal.

A POSSIBILIDADE DE USO DE *MALWARE* EM INVESTIGAÇÕES CRIMINAIS ESTÁ PREVISTA NO N.º 2 DO ARTIGO 19.º DA LEI DO CIBERCRIME?

Todavia, recentemente, têm surgido alguns Autores a sufragar que o aludido n.º 2 do artigo 19.º da Lei do Cibercrime consagraria, na verdade, a possibilidade de utilização de *malware* para realização de acções encobertas de investigação criminal em sistemas informáticos, isto é, buscas *on-line*.

De facto, o n.º 2 do artigo 19.º da Lei do Cibercrime dispõe o seguinte: "*Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações*".

Apesar de reconhecerem que o n.º 2 do artigo 19.º da Lei do Cibercrime constitui uma disposição formulada em termos "*muitíssimo vagos*", há Autores que entendem que esta norma já consagraria a possibilidade de utilização de *malware* em investigações criminais para realização de *buscas on-line* encobertas.

Com efeito, e de acordo com a aludida interpretação, o n.º 2 do artigo 19.º da Lei do Cibercrime não poderia, nas palavras de David Silva Ramalho, "*constituir uma previsão redundante e supérflua que visasse tão-somente permitir ao agente encoberto recorrer a quaisquer outros meios e dispositivos informáticos previstos na lei processual penal*" (Métodos Ocultos de Investigação Criminal em Ambiente Digital, 2017, Almedina, páginas 344 e 345).

5 Por exemplo: a criação de uma identidade digital fictícia para monitorizar a actividade de um suspeito num determinado chat *on line*.

Deste modo, a expressão "*meios e dispositivos informáticos*" constante do n.º 2 do artigo 19.º da Lei do Cibercrime apenas poderia significar, no entender de David Silva Ramalho, "*meios e dispositivos que operem de modo materialmente semelhante à figura do agente encoberto - em particular ao agente encoberto em ambiente digital - e que devam ser utilizados quando a própria acção encoberta e dos demais métodos ocultos forem incapazes de dar resposta às exigências da investigação. Trata-se, a nosso ver, da consagração do hacking e da utilização (que incluirá, naturalmente, a instalação) de malware como método oculto de investigação criminal em ambiente digital*" (Métodos Ocultos de Investigação Criminal em Ambiente Digital, 2017, Almedina, página 346).

No mesmo sentido, também João Conde Correia sufraga que "*as buscas online resultam da possibilidade de recorrer a meios e dispositivos informáticos no decurso de acções encobertas*" ("Prova digital: as leis que temos e a lei que devíamos ter", *in Revista do Ministério Público*, n.º 139, Setembro 2014, página 43).

Segundo David Silva Ramalho, a possibilidade de se recorrer ao *malware* no âmbito de uma investigação criminal, ao abrigo do disposto no n.º 2 do artigo 19.º da Lei do Cibercrime, encontrar-se-ia sujeita a um regime jurídico que tem de ser "*encontrado simultaneamente nas normas relativas às acções encobertas e à intercepção de comunicações da Lei do Cibercrime, no regime jurídico das acções encobertas, aprovado pela Lei n.º 101/2001, acima analisado, e no regime das escutas telefónicas previsto no CPP*" (Métodos Ocultos de Investigação Criminal em Ambiente Digital, 2017, Almedina, página 346).

De acordo com este Autor, as principais directrizes do regime jurídico relativo à possibilidade de uso de *malware* seriam as seguintes:

— O uso de *malware* apenas seria admissível quando existissem fundadas suspeitas da prática dos crimes previstos no catálogo previsto no n.º 1 do artigo 19.º da Lei do Cibercrime;

— O uso de *malware* apenas seria admissível num quadro de facto em que as acções encobertas sejam adequadas aos fins de repressão criminais identificados em concreto e sejam proporcionais a essas finalidades, bem como à gravidade do crime em investigação (cfr. artigo 3.º da Lei n.º 101/2001);

— O uso de *malware* não seria admissível em acções encobertas de natureza preventiva, mas apenas no decurso de um inquérito criminal (cfr. n.º 2 do artigo 18.º da Lei do Cibercrime, aplicável ex parte final do n.º 2 do artigo 19.º do mesmo diploma);

— O uso de *malware* só poderia ser autorizado se houver "*razões para crer que a diligência é indispensável para a descoberta da verdade material ou que a prova seria, de outra forma, impossível ou muito difícil de obter*" (cfr. n.º 2 do artigo 18.º da Lei do Cibercrime, aplicável ex parte final do n.º 2 do artigo 19.º do mesmo diploma);

— O uso de *malware* apenas poderá ser autorizado por "*despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público*" (cfr. n.º 2 do artigo 18.º da Lei do Cibercrime, aplicável ex parte final do n.º 2 do artigo 19.º do mesmo diploma);

— A autorização para o uso de *malware* deverá definir o âmbito concreto da diligência de investigação (cfr. n.º 3 do artigo 18.º da Lei do Cibercrime, aplicável ex parte final do n.º 2 do artigo 19.º do mesmo diploma);

— O recurso ao *malware* deve constar dos autos de inquérito, por força do disposto no n.º 8 do artigo 188.º do CPP, aplicável ex vi n.º 4 do artigo 18.º da Lei do Cibercrime;

— O uso de *malware* não pode ser utilizado para activar o *hardware* de captação de imagem e som do sistema informático infectado.

Não obstante admitir que a possibilidade de uso de *malware* se encontra consagrada no n.º 2 do artigo 19.º da Lei do Cibercrime, David Silva Ramalho não deixa de considerar que o regime aplicável ao *malware* "*é manifestamente inadequado para regular aquele que, ao que tudo indica, será o meio de obtenção de prova mais invasivo e intensamente restritivo de direitos fundamentais consagrados na lei processual penal portuguesa*" (Métodos Ocultos de Investigação Criminal em Ambiente Digital, 2017, Almedina, página 351).

Em primeiro lugar, considerando o elevado nível de danosidade social do uso de *malware*, David Silva Ramalho admite que o n.º 2 do artigo 19.º da Lei do Cibercrime não regula de forma clara, precisa e previsível os pressupostos e condições de utilização do *malware*, razão pela qual seria inconstitucional por violação das disposições conjugadas dos artigos 18.º, n.º 2, 26.º, n.º 2, e 1.º da CRP.

Em segundo lugar, o facto de o legislador não ter definido que tipo de dados se pode apreender através do uso de *malware* e com que finalidade também suscitaria dúvidas de conformidade constitucional.

Em terceiro lugar, o catálogo de crimes excessivamente amplo para o uso de *malware* e que inclui ilícitos criminais com pena máxima abstractamente aplicável de três anos também suscita, no entender de David Silva Ramalho, "*questões de proporcionaldidade, não só pela sua reduzida gravidade mas também porque, sendo o uso de malware um meio excepcional dentro de outro meio excepcional* [acções encobertas]*, deveria a sua utilização estar sujeita a um catálogo mais restrito*" (Métodos Ocultos de Investigação Criminal em Ambiente Digital, 2017, Almedina, páginas 351 e 352).

Em quarto lugar, a duração temporal do recurso ao *malware* – prazo de três anos, renovável por iguais períodos, por aplicação do regime aplicável às escutas telefónicas (cfr. n.º 4 do artigo 18.º da Lei do Cibercrime, aplicável *ex vi* n.º 2 do artigo 19.º do mesmo diploma) – também "*não deveria, em virtude do princípio da subsidiariedade na aplicação de métodos ocultos, ser igual ao regime aplicável às escutas telefónicas*" (Métodos Ocultos de Investigação Criminal em Ambiente Digital, 2017, Almedina, página 352).

Em suma, apesar de alguns Autores entenderem que o n.º 2 do artigo 19.º da Lei do Cibercrime já consagraria a possibilidade de se recorrer a *malware* no âmbito de acções encobertas, não deixam - em particular David Silva Ramalho - de reconhecer que o regime (alegadamente) estipulado pelo legislador penal nesta matéria não deixa de suscitar "*mais questões do que aquelas que* resolve[m] *e* gera[m] *uma sombra de incerteza quanto à admissibilidade e contornos deste meio de obtenção de prova que são incompatíveis com a sua gravidade*" (Métodos Ocultos de Investigação Criminal em Ambiente Digital, 2017, Almedina, páginas 354 e 355).

A POSSIBILIDADE DE USO DE *MALWARE* EM INVESTIGAÇÕES CRIMINAIS ESTÁ PREVISTA NO ARTIGO 15.º DA LEI DO CIBERCRIME?

Outros Autores, como Paulo Pinto de Albuquerque, sufragam que o legislador penal teria consagrado a possibilidade de as autoridades de investigação criminal recorrerem a *malware* e realizarem *buscas on line* nos sistema informáticos dos visados no artigo 15.º da Lei do Cibercrime.

Nas palavras de Paulo Pinto de Albuquerque: "*A busca on line consiste na infiltração electrónica em sistemas informáticos, por exemplo, através dos chamados cavalos de Tróia, de modo a que o investigador possa em tempo real ou deferido conhecer a informação que está a ser introduzida ou já foi introduzida no sistema, incluindo textos, sons e imagens. A busca on line não é admissível, no direito português, como meio atípico de obtenção de prova, desde logo dado o seu carácter ilícito. Atento o seu elevado grau de intrusão na privacidade do suspeito, este meio de obtenção de prova deve ser previsto por uma lei expressa e exige reserva de competência judicial (…). A busca on line foi agora consagrada pelo novo artigo 15.º da Lei n.º 109/2009, de 15.9, que prevê a «pesquisa em sistema informático»*" (Comentário do Código de Processo Penal, 2011, Universidade Católica Editora, página 502).

Não obstante entender que o legislador teria consagrado as *buscas on line* no artigo 15.º da Lei do Cibercrime, Paulo Pinto de Albuquerque considera que esta norma seria inconstitucional. Na verdade, Paulo Pinto de Albuquerque entende que o artigo 15.º da Lei do Cibercrime permite, por um lado, que as pesquisas informáticas sejam ordenadas por despacho da autoridade judiciária ou mesmo decisão do órgão de polícia criminal (sem sequer ser necessário a validação por um juiz) e, por outro, não coloca quaisquer restrições relativamente ao conteúdo dos dados que podem ser pesquisados.

Assim, Paulo Pinto de Albuquerque sufraga que o artigo 15.º da Lei do Cibercrime é inconstitucional por constituir uma "*intrusão na privacidade da pessoa visada*" que seria "*manifestamente desproporcional, em face do artigo 26.º, n.os 1 e 2, e do 32.º, n.º 4, da CRP, que reservam ao juiz os actos instrutórios que representem uma intrusão na privacidade. Assim, o artigo 15.º da Lei n.º 109/2009, seria inconstitucional, na medida em que permite que o MP e o OPC ordenem a pesquisa de um sistema informático, incluindo dados informáticos íntimos ou privados, sem o controlo prévio ou posterior da «pesquisa» por um juiz*" (Comentário do Código de Processo Penal, 2011, Universidade Católica Editora, página 502).

No entanto, segundo Paulo Pinto de Albuquerque, a única forma de fugir ao juízo de inconstitucionalidade do artigo 15.º da Lei do Cibercrime seria a de submeter os dados informáticos íntimos ou privados ao juiz e este validar a pesquisa por aplicação do disposto no n.º 3 do artigo 16.º da Lei do Cibercrime.

Em suma, também há quem veja a consagração da possibilidade de uso de *malware* para realização de *buscas on line* no artigo 15.º da Lei do Cibercrime, embora também levantando dúvidas quanto à constitucionalidade do regime.

A RESERVA DA LEI E A (IM)POSSIBILIDADE DE O USO DE *MALWARE* TER SIDO CONSAGRADO NA LEI DO CIBERCRIME

Não obstante as posições acima referidas - que admitem que o recurso ao *malware*, enquanto meio de investigação oculto, já se encontraria consagrado na Lei do Cibercrime (seja por via do artigo 15.º, seja por via do n.º 2 do artigo 19.º) -, sufragamos que o uso do *malware* ainda não se encontra legalmente previsto, razão pela qual, à luz do Direito constituído, qualquer prova recolhida através deste método de investigação oculto constituirá prova nula, nos termos do disposto no artigo 126.º do CPP.

Em primeiro lugar, através da análise dos trabalhos preparatórios da Lei do Cibercrime, resulta que a vontade do legislador penal não foi a de consagrar a possibilidade do uso de *malware* como método de investigação oculto na Lei do Cibercrime.

Aliás, na discussão na generalidade da proposta da Lei do Cibercrime, o Deputado Fernando Negrão perguntou o seguinte: "*Por que é que não foi contemplada neste diploma a possibilidade de as entidades de investigação criminal introduzirem em determinado sistema que esteja sob investigação o que podemos designar por «cavalo de Tróia informático», para poder obter informação contínua e em tempo real, assim facilitando as investigações criminais, designadamente através dos meios informáticos?*" (DAR I série n.º 102/X/4 2009.07.10, página 40).

Note-se que a Lei do Cibercrime acabou por ser aprovada com os mesmos termos e condições daqueles que constavam na proposta de lei que suscitou a pergunta do Deputado Fernando Negrão.

Ora, a interpretação da lei processual penal não tem, em bom rigor, autonomia, pelo que são aplicáveis os critérios previstos no artigo 9.º do Código Civil, em particular a necessidade de reconstituir, a partir dos textos, o pensamento legislativo, designadamente através das circunstâncias em que a lei foi elaborada e as específicas condições de tempo da sua aplicação.

Nas palavras de Simas Santos e Leal Henriques: "*Tanto que o Código de Processo Penal não contempla a matéria de interpretação, o que nos remete, obviamente, para a doutrina geral de interpretação de leis, desde logo para os critérios inscritos no art.º 9.º do Código Civil*" (Noções de Processo Penal, 2011, Rei dos Livros, página 61).

Assim sendo, e recorrendo aos trabalhos preparatórios, conclui-se que, ao que tudo indica, o legislador penal jamais pretendeu - pelo menos, intencionalmente - consagrar a figura do *malware* – enquanto meio de investigação oculto – na Lei do Cibercrime.

Em segundo lugar, o artigo 15.º da Lei do Cibercrime prevê, conforme se referiu *supra*, a pesquisa de dados informáticos, o que, como sustenta Pedro Verdelho, "*mais não é que uma busca no ambiente digital*" ("Lei do Cibercrime", *in Scientia Juridica*, Tomo LVIII, n.º 320, 2009, página 740).

Como explica Pedro Verdelho: "*...será completamente errado ver nesta figura algum tipo de substituto para os exames, clássicos meios de obtenção de prova, previstos nos arts. 171.º e segs. do Código de Processo Penal (CPP). Aliás, a lei é clara e expressa, dizendo que a esta diligência são aplicáveis (...) as regras de execução das buscas previstas no Código de Processo Penal*" ("Lei do Cibercrime", *in Scientia Juridica*, Tomo LVIII, n.º 320, 2009, página 740).

Deste modo, o artigo 15.º da Lei do Cibercrime não consagra a possibilidade de se recorrer a meios ocultos de investigação criminal como é o caso do *malware*, mas apenas a faculdade de realizar buscas em sistemas informáticos (e não a monitorização de sistemas informáticos em tempo real).

Em terceiro lugar, o n.º 2 do artigo 19.º da Lei do Cibercrime limita-se, em nossa opinião, a estatuir, porventura de forma tautológica e através de uma redacção pouco feliz, que os agentes encobertos têm a faculdade de recorrer a quaisquer outros meios e dispositivos informáticos previstos na lei processual penal, caso em que há que respeitar as regras previstas para a intercepção de comunicações prevista no artigo 18.º da Lei do Cibercrime. Como explica Benjamim da Silva Rodrigues: "*...sempre que se afigure necessário o recurso a meios e dispositivos informáticos, sob pena de proibição de valoração dessa prova, há que respeitar as regras impostas para a intercepção de comunicações*" (Da Prova Penal, Tomo II, Rei dos Livros, 1.ª Edição, 2010, página 456).

Portanto, salvo melhor opinião, o n.º 2 do artigo 19.º da Lei do Cibercrime também não consagra a admissibilidade do recurso a *malware* como meio oculto de investigação criminal.

Em quarto lugar, e conforme se referiu *supra*, é inegável que os meios ocultos de investigação criminal - como é o caso do recurso ao *malware* - encontram-se sujeitos a uma incontornável reserva de lei, só sendo admissíveis aqueles que gozam de expressa e específica consagração legal.

Nas palavras de Costa Andrade: "*configurando inevitavelmente um sacrifício de direitos fundamentais, os*

meios ocultos de investigação criminal começam por estar sujeitos - e este é um dos esteios irredutíveis do respectivo regime geral - a uma intransponível reserva de lei. Só são admissíveis e válidos se e na medida em que gozam de expressa e específica consagração legal" ("Métodos ocultos de investigação (Plädoyer para uma teoria geral)", *in Que futuro para o Direito Processual Penal?*, 2009, Coimbra Editora, página 540).

E, para além de ser expressa, a consagração legal de um método oculto de investigação criminal - dado o potencial de agressividade relativamente a direitos fundamentais - tem também, nas palavras de Costa Andrade, "*de prever expressa e explicitamente a medida de compressão de direitos fundamentais, fixar a sua compreensão, extensão e vinculação finalístico-teleológica bem como definir os seus limites*" ("Métodos ocultos de investigação (Plädoyer para uma teoria geral)", *in Que futuro para o Direito Processual Penal?*, 2009, Coimbra Editora, página 541).

Assim sendo, é evidente que, por força das exigências decorrentes do princípio da reserva de lei, jamais se poderia concluir, salvo melhor opinião, que a Lei do Cibercrime consagraria o uso de *malware* como meio oculto de investigação criminal, na medida em que inexiste aí qualquer norma que preveja expressa e explicitamente a possibilidade de recurso a *malware*[6].

Aliás, a prova de que não há nenhuma norma que, expressa e explicitamente, consagre o *malware* na Lei do Cibercrime é que, conforme se viu *supra*, quem entende que este meio oculto de obtenção de prova já se encontraria vertido na Lei do Cibercrime não está sequer de acordo em relação à norma que concretamente consagraria a figura (para uns o artigo 15.º; para outros o n.º 2 do artigo 19.º, ambos da Lei do Cibercrime).

Tanto mais que a utilização de *malware* é, naturalmente, um meio oculto de obtenção de prova substancialmente danoso ao nível de direitos fundamentais, na medida em que o acesso, em tempo real, aos sistemas informáticos do visado coloca em causa o direito à reserva da intimidade da vida privada, o direito à palavra escrita e falada, o direito à autodeterminação informacional, o direito à inviolabilidade do sigilo das comunicações electrónicas, o direito à inviolabilidade dos dados de carácter pessoal, etc.

Aliás, há doutrina que equipara os sistemas informáticos ao "*domicílio digital*" do proprietário/utilizador. Como explica Benjamim da Silva Rodrigues: "*O computador surge-nos, cada vez com maior insistência e persistência, como o «domicílio informático» ou a «casa digital» onde mora a nossa «alma digital» cujo desapossamento poderá configurar uma irremediável «falsificação existencial»*" (Da Prova Penal, Tomo II, Rei dos Livros, 1.ª Edição, 2010, página 473). Deste modo, a possibilidade de se recorrer ao *malware* como meio oculto de investigação criminal constituiria, na verdade, uma compressão do direito à inviolabilidade do domicílio.

À luz do exposto, parece certo que o sistema processual penal Português não prevê a possibilidade de se recorrer ao uso de *malware* como método oculto de investigação criminal.

Como explica Benjamim da Silva Rodrigues: "*mais uma vez, para desgosto de alguns, haverá que afirmar que este método oculto de investigação não tem expressa consagração no ordenamento jurídico português. De facto, por força dos artigos 18.º, n.º 2, 34.º, n.º 4 e 35.º, n.º 4, haverá que adoptar uma lei expressa, clara e determinada que permita, apenas em situações forçosamente gravosas, dada a elevada danosidade e perturbação múltipla de diversos e diferenciados direitos fundamentais, a busca online*" (Da Prova Penal, Tomo II, Rei dos Livros, 1.ª Edição, 2010, página 474).

Iure condendo - A possibilidade de recurso a *malware* para situações de terrorismo e criminalidade altamente organizada e perigosa (notas breves)

Compreende-se que, no actual contexto digital, seja fundamental que a investigação criminal dis-

6 No ordenamento jurídico Espanhol, o artigo 588.º, *septies a*, da Ley de Enjuiciamento Criminal permite o recurso a *malware* de forma clara e cristalina em obediência ao princípio da reserva de lei. De facto, o n.º 1 do mencionado artigo 588.º estabelece o seguinte: "*El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos*". Contudo, o recurso ao *malware* apenas está autorizado quando estiverem causa os seguintes crimes: a) Crimes cometidos por organizações criminais; b) Terrorismo; c) Crimes contra menores ou inabilitados; d) Crimes contra a Constituição e relativos à defesa nacional; e) Crimes cometidos através de instrumentos informáticos ou serviço de comunicação. A decisão judicial que autorizar o recurso ao *malware* deverá: (i) especificar o objecto do *malware* (quais os sistemas informáticos que deverão ser infectados); (ii) especificar o alcance do recurso ao *malware* e a forma que o mesmo revestirá; (iii) especificar os agentes autorizados para a execução da operação encoberta de uso de *malware*; (iv) autorizar a realização e conservações de cópias de dados informáticos; (v) especificar as medidas para preservação dos dados armazenados.

ponha de meios eficientes de obtenção de prova em ambiente digital. Todavia, e conforme resulta do *supra* exposto, o recurso ao *malware* para realização de acções encobertas de obtenção de prova, dado o seu carácter invasivo e intensamente restritivo de direitos fundamentais, deve ser absolutamente excepcional, dispondo de um regime próprio e sendo apenas admissível para casos de terrorismo ou criminalidade altamente organizada e perigosa.

Caso contrário - isto é, se a possibilidade de recurso ao *malware* não for absolutamente excepcional e restringida aos casos acima referidos -, será, em nossa opinião (mais) um passo na direcção do pesadelo totalitário de George Orwell: "*Big Brother is watching you*".

CONCLUSÃO

À luz da legislação vigente, o recurso ao *malware* enquanto meio oculto de investigação criminal não é, salvo melhor opinião, permitido no sistema processual penal Português (designadamente, na Lei do Cibercrime). Assim sendo, e salvo melhor opinião, à luz do direito constituído, quaisquer provas eventualmente obtidas através da utilização de *malware* serão nulas, por força do artigo 126.º, n.os 1 e 2, do CPP.

Por fim, e em termos de *iure condendo*, entendemos que o recurso ao *malware* para realização de acções encobertas de obtenção de prova deve ser absolutamente excepcional, dispondo de um regime próprio e sendo apenas admissível para casos de terrorismo ou criminalidade altamente organizada e perigosa.