# O USO DE *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA EM PROCESSO PENAL[1]

*David Silva Ramalho*[2]

Abstract: *The use of malware as means of obtaining evidence has increased in the course of the past years due to its effectiveness to counter the anti-forensic measures adopted by cybercriminals. In Portugal, we believe that this investigatory tool was inserted in the Cybercrime Law as a technological device to be used in undercover operations. However, the terms in which this provision was foreseen lack clarity, precision and most of all respect for the defendant's rights, thus raising doubts as to its constitutionality.*



---

1 O artigo que ora se apresenta encontra-se atualizado com elementos factuais e bibliográficos até outubro de 2013.

2 Advogado, Investigador no Centro de Investigação em Direito Penal e Ciências Criminais da Faculdade de Direito da Universidade de Lisboa e Fellow no Tech and Law Center de Milão. Contacto do autor: dsr@servulo.com.

## INTRODUÇÃO

### 1. Apresentação do problema

Com a aprovação da Lei n.º 109/2009, de 15 de setembro, a Lei do Cibercrime, o legislador português criou um dispositivo processual que, em rigor, nunca foi explicado e cujo significado permanece por esclarecer.

A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias não se lhe referiu no seu parecer sobre a Proposta de Lei n.º 289/X (4.ª), o Parlamento aprovou-o sem qualquer voto contra na especialidade, a jurisprudência dos tribunais superiores – tanto quanto sabemos – nunca se lhe referiu e a doutrina raramente se pronuncia sobre ela, limitando-se, quando o faz, a transcrevê-la ou a questionar-se sobre o seu alcance.

Referimo-nos à última norma do capítulo dedicado às disposições processuais da Lei do Cibercrime, o artigo 19.º, n.º 2, subordinado à epígrafe "*ações encobertas*" e que reza o seguinte: "[s]*endo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações*".

Da leitura do referido preceito decorre, desde logo, uma questão: o que são estes "*meios e dispositivos informáticos*"? Estar-se-á, como sugere Paulo Dá Mesquita, "*por esta via, a abrir-se, sem suficiente ponderação (ou freios claros) a porta à interceção de comunicações para fins de prevenção*"[3]? Ou será que a remissão feita por aquela norma para "*as regras previstas para a interceção de comunicações*" visa, precisamente, afastar a qualificação destes "*meios e dispositivos informáticos*" como verdadeira *interceção de comunicações*, nos termos do artigo 18.º da Lei do Cibercrime, e qualificá-los antes como um meio de obtenção de prova *análogo* à interceção de comunicações? Um entendimento desta natureza coloca no intérprete – leia-se, no jurista não letrado em tecnologias de informação – uma dificuldade de densificação normativa do conceito de "*meios e dispositivos informáticos*". Dificuldade que, por impulso ou desconforto, tende a ser remetida para o acervo de conceitos técnicos comummente entendidos como exteriores ao Direito.

A questão que ora se formula é simples, embora não o seja a resposta a dar-lhe, e é ela que lançará o mote para o presente estudo: será admissível, à luz

3 Mesquita, 2010: 127.

do quadro legal e constitucional vigente em Portugal, a utilização de *malware* como meio de obtenção de prova em processo penal[4]?

Como decorre desta formulação, o problema terá de ser analisado em duas vertentes: a primeira, dedicada à procura da eventual existência de base legal no quadro jurídico vigente para fundamentar o recurso a este meio de obtenção de prova; a segunda, fazendo passar pelo crivo da constitucionalidade o recurso ao *malware*, procurando aferir dos requisitos e pressupostos da sua aplicabilidade e da respetiva conformidade com a Lei Fundamental.

O nosso objetivo com o presente estudo é, principalmente, o de suscitar estas questões perante a comunidade científica, oferecendo, de forma sintética e necessariamente introdutória, a nossa visão sobre o assunto, reservando o seu desenvolvimento para momento posterior.

## 2. Razão de ordem

Para uma resposta adequada à questão formulada, optámos por uma análise tripartida do problema: a primeira fase de pendor técnico, a segunda de cariz histórico-comparatístico e a terceira de análise jurídica ao nível do direito interno.

Contudo, antes de iniciarmos o nosso trajeto expositivo, procurando delimitar as coordenadas fácticas e técnicas do *malware*, haverá que alertar o leitor para o facto de que as definições apresentadas não são unânimes ou estáticas

---

4 Esta foi simultaneamente a primeira e a última questão a ser colocada na discussão na generalidade da Proposta de Lei n.º 289/X (4.ª), embora aí apenas se tenham referido os chamados cavalos de Tróia. Da primeira vez, o Deputado Fernando Negrão, do PSD, imediatamente após o início da discussão parlamentar na generalidade, formulou-a do seguinte modo: "[p]*or 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?*". Não tendo obtido resposta, já no fim da discussão parlamentar, insistiu o mesmo Deputado do seguinte modo: "*Sr. Presidente, é apenas para reiterar as perguntas que formulei, mas a que o Sr. Secretário de Estado não respondeu. A primeira era a de saber o porquê da repetição da figura da associação criminosa neste diploma. Perguntei qual era a lógica de, de diploma em diploma, entramos num processo de repetição da figura da associação criminosa, mas o Sr. Secretário de Estado não respondeu. Em segundo lugar, perguntei o seguinte: por que não a criação de um novo tipo legal de crime, que facilitaria a investigação criminal, no sentido de introduzir 'cavalos de Tróia' informáticos nos sistemas informáticos, para facilitar a investigação criminal? Era só para registar que o Sr. Secretário de Estado não respondeu a qualquer destas perguntas*". A resposta surgiu do seguinte modo: "*O Sr. Presidente (Nuno Teixeira de Melo): – Sr. Deputado, o Sr. Secretário de Estado também já não dispõe de tempo para responder. Talvez possa fazê-lo noutra altura, porventura na sequência dos trabalhos em sede de especialidade, se for caso disso.*". Na discussão na especialidade, a questão, tanto quanto sabemos, não foi colocada e a norma veio a ser aprovada com os votos da bancada do PSD, do PS e do CDS-PP e a abstenção do PCP e do BE – cf. DAR II série A N.º.167/X/4 2009.07.27.

e tão-pouco são destituídas de ocasionais sobreposições conceptuais. Tal facto decorre das mutações a que o *software* malicioso é constantemente sujeito e da inexistência de acordo, por parte da doutrina especializada, quanto às características a atribuir a cada tipo de *malware*.

Não obstante inexista unanimidade quanto aos conceitos, às especificidades e aos limites das diversas categorias de *malware*, a verdade é que para a correta apreensão do problema se nos afigura particularmente relevante encetar um esforço no sentido da apresentação de noções básicas a partir das quais possamos apreender as características e modo de funcionamento de cada uma das modalidades deste meio técnico. Desde logo porque, segundo cremos, para uma correta análise da adequação de um meio de obtenção de prova digital, o jurista não pode conformar-se com o seu desconhecimento em matérias não-jurídicas, mas deverá antes procurar compreender o seu funcionamento e enquadrá-lo à luz dos preceitos legais e constitucionais vigentes. Assim, e sem prejuízo de ser ao perito que cabe explicar os factos de acordo com os seus especiais conhecimentos técnicos e científicos, é ao jurista que cabe aferir da legalidade do meio utilizado para recolha da informação sobre a qual a perícia eventualmente incidirá.

Uma vez delimitadas as coordenadas iniciais, haverá, então, que proceder à análise da origem e evolução da utilização de *malware* como ferramenta de investigação criminal em ambiente digital. Para tal, começar-se-á por uma breve análise do sistema norte-americano, onde, tanto quanto se sabe, teve origem a utilização de *malware* como ferramenta de suporte à investigação criminal. De seguida proceder-se-á a uma breve análise do sistema alemão, com particular incidência na decisão do Tribunal Constitucional Federal (*Bundesverfassungsgericht*) sobre a utilização de *malware* e no funcionamento do chamado *Bundestrojaner* e, subsequentemente, analisar-se-á o regime espanhol, onde se encontra atualmente em discussão o anteprojeto de Código de Processo Penal que, entre outros objetivos, visa esclarecer as fundadas dúvidas existentes sobre a admissibilidade do recurso a esta tecnologia. O capítulo terminará com uma análise sobre a tendência para a consagração do *malware* como ferramenta de investigação criminal, em particular nos países das Caraíbas e da União Europeia, fruto de iniciativas de cariz supranacional.

O último capítulo, pressupondo já algumas noções das coordenadas técnicas do *malware* e as experiências em ordenamentos jurídicos distintos, visa oferecer uma breve e sumária análise jurídica sobre a eventual suficiência das previsões

legais ao nível processual penal português para a admissibilidade deste meio de obtenção de prova e uma subsequente densificação dos requisitos e pressupostos que, inevitavelmente, teriam de sustentar semelhante entendimento.

## 3. Delimitação conceptual

Para uma correta compreensão da realidade do cibercrime e das especificidades da prova digital, há que reconhecer que, com o advento da Internet e a incessante evolução tecnológica, surgiram novas realidades que não são subsumíveis aos conceitos até então existentes. Quando assim sucede, há que fazer uma opção metodológica: ou se adaptam os conceitos já existentes para abrangerem as novas realidades – com o possível desvirtuamento do seu significado inicial por via do esbatimento dos seus contornos – ou se importam conceitos novos de outras áreas do saber e se lhes atribui uma configuração jurídica.

O legislador e a doutrina propendem para a primeira das opções. E apesar de a Lei do Cibercrime ser, em geral, uma exceção a esta tendência, a verdade é que não lhe é totalmente imune. Tal facto é evidenciado, quanto ao legislador, pela circunstância de na Lei do Cibercrime ter submetido acriticamente as ações encobertas em ambiente digital ao regime das ações encobertas previstas na Lei n.º 101/2001, de 15 de agosto, e, quanto à doutrina, no que aqui releva, qualificando como busca *online*[5] a utilização de *malware* como meio oculto de investigação criminal.

Quanto a nós, porquanto entendemos que se trata de um conceito novo no plano jurídico e que merece destacamento de outros conceitos com contornos e propósitos diferentes, optámos por nos referir exclusivamente ao conceito de *malware*, ou a cada uma das suas subespécies, nas suas vertentes de instalação, de pesquisa e de recolha de informação e não – salvo quando estritamente necessário – ao de *busca online*. E fizemo-lo essencialmente por dois motivos: por um lado, porque não se trata aqui de uma busca – pelo menos não mais do que uma escuta telefónica se traduz numa busca telefónica – e, por outro, porque tão pouco é necessário que a instalação de *malware* ou a recolha de informação por este *software* ocorra *online*.

---

5 Costa Andrade define as buscas *online* como "*um conceito compreensivo e abrangente, porventura mesmo não inteiramente rigoroso, a que se reconduz um conjunto de intromissões nos sistemas informáticos, feitas através da internet e que se atualizam na observação, busca, cópia, vigilância, etc., dos dados presentes naqueles sistemas informáticos*", cf. Andrade, 2009a: 166.

Quanto à primeira objeção, começar-se-á por referir que a remissão genérica para o conceito de busca, na medida em que se encontra desacompanhada do vocábulo *domiciliária*, pareceria levar a que se admitisse a suficiência da mera precedência de autorização por despacho do Ministério Público para a sua realização, nos termos do disposto no artigo 174.º do CPP – o que a privaria da necessária reserva de juiz. Por outro lado, caso se compare a busca *online* a uma busca domiciliária[6] – o que, quanto a nós, é destituído de acuidade jurídica –, a verdade é que se estará a descaracterizar o conceito de *domicílio* e o fundamento que subjaz à proteção acrescida atribuída ao visado por esta medida pela norma do artigo 177.º[7], até porque o *malware* pode ser instalado em telemóveis, em computadores portáteis ou em *tablets*, onde quer que os mesmos se encontrem.

Acresce que, numa busca *online*, o investigador pode monitorizar toda a atividade do visado *em direto*, ativando, se necessário, a sua *webcam* ou o microfone do sistema informático infetado e assistindo, se necessário, à prática de ilícitos em tempo real sem o conhecimento do visado – contrariamente ao que sucede numa busca.

Quanto à segunda das objeções enunciadas, e como as ferramentas de ciberespionagem *Flame* e *Stuxnet*[8] vieram demonstrar, o *malware* pode ser instalado num computador desligado da Internet através de um suporte digital removível – designadamente via USB –, apreendendo de seguida os dados pretendidos (*offline*) para, por fim, transportá-los para outra unidade removível até finalmente chegar a um sistema informático conectado à Internet, a partir do qual os remeterá ao seu controlador.

---

6 A este respeito, e a par da comparação do computador à *alma digital*, Benjamim Silva Rodrigues alude à ideia de domicílio informático-digital em matéria de buscas *online* – cf. Rodrigues, 2010: 472-473.

7 Sobre este assunto, sustenta Costa Andrade o seguinte: "*Pacífico em qualquer caso que ela não está coberta pelas normas processuais penais que legitimam a violação do domicílio, no contexto da clássica figura das* buscas." - Andrade, 2009a: p. 168.

8 Por se tratar de ferramentas de ciberespionagem, não nos pronunciaremos no presente estudo sobre o *Stuxnet* e o *Flame*, nem sobre o *Duqu* ou o *Gauss*. Todavia, sendo estes os tipos de *malware* mais avançados alguma vez descobertos, supostamente financiados por Estados e não por entidades privadas, afigura-se-nos pertinente referir as suas propriedades, uma vez que poderão vir a ser adaptadas para o contexto da investigação criminal. Para uma análise do *Stuxnet* v., por todos, a compilação de informação efectuada pelo *Federal Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT), disponível em: http://www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf [consultado em: 03-10-2013]. Para uma breve análise descritiva do *Stuxnet* e do *Flame* v. Morton & Grace, 2012. Por fim, para uma descrição e comparação entre o *Flame*, o *Stuxnet*, o *Gauss* e o *Duqu*, cf. Gradigo, 2013: 47-52.

Por fim, cumpre referir apenas que, segundo cremos, o termo "*busca online*" encontra a sua origem no debate jurisprudencial ocorrido no direito norte-americano sobre a eventual subsunção da utilização de *malware* para fins de investigação criminal ao conceito de busca (*search*), previsto na Quarta Emenda à Constituição dos EUA, o que releva, naquele ordenamento, para aferição da eventual necessidade de precedência de mandado judicial para a sua utilização[9]. O termo perde pertinência quando entramos no léxico constitucional português e, como tal, deverá merecer tratamento independente da carga valorativa que lhe advém daquele ordenamento, com a devida autonomia em face de um meio de obtenção de prova que não lhe é comparável[10].

Assim, e porquanto se nos afigura como a expressão tecnicamente mais rigorosa, optámos por nos referir sempre, ao longo do presente estudo, ao termo *malware*, e não a *busca online*.

## CAPÍTULO I – *MALWARE*

### 1. Noção e modalidades

O termo *malware* é o resultado da contração do adjetivo *malicious* (malicioso) e do substantivo *software* (programa informático)[11] e pode ser definido resumidamente como "*um conjunto de instruções executadas no computador que levam o sistema a fazer algo que um atacante quer que ele faça*"[12] ou, mais desenvolvidamente, como "*um programa simples ou auto-replicativo que discretamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade*

9 Esta questão começou por ser colocada a propósito das escutas telefónicas e viria a ser resolvida no sentido da sua subsunção ao conceito de busca no caso *Charles Katz v. United States* – sobre este caso, v. Landau, 2010: 70 e Garitaonandia, 2010: 337-339. O problema veio a reactivar-se com a questão da eventual subsunção das interceções de comunicações e do recurso a *malware* no contexto das investigações criminais em ambiente digital, tendo recebido, em geral, entendimento idêntico ao das escutas, isto é, no sentido da necessidade de mandado prévio à sua utilização – cf. Brenner, 2012: 81.

10 A menos que, na esteira de Buermeyer entendamos que, ao entrar no computador de alguém, "*o Estado como que põe o pé virtual na porta da sua casa*" – *apud* Andrade, 2009a: 167. A este respeito cumpre recordar que o enquadramento legal que parte da doutrina alemã fazia das ditas buscas *online* no regime das tradicionais buscas foi rejeitado pelo BGH na sua decisão de 31 de janeiro de 2007 – cf. Pradillo, 2009: 3.

11 Não ignoramos que poderá causar estranheza a utilização da expressão *malicioso* para um instrumento utilizado por órgãos de polícia criminal no contexto da sua atividade de investigação criminal, cujo objetivo último é a realização da Justiça. Todavia fazemo-lo sem qualquer carga valorativa sobre a referida atividade, mas antes porque se trata de um termo genérico que engloba vários tipos de *malware*, bem como porque é um tipo de *software* que é intrusivo, insidioso e, portanto, malicioso em relação ao sistema informático no qual se instala.

12 Boldt, 2010: 10.

*dos dados, a integridade dos dados e a disponibilidade do sistema ou para assegurar que o utilizador seja incriminado por um crime informático*"[13].

Como decorre de ambas as definições, o conceito de *malware* reveste-se de uma amplitude significativa. Em síntese, inclui todo o tipo de programas instalados sub-repticiamente por terceiros num sistema informático que podem ser utilizados para, de algum modo, comprometer as suas funções, contornar os seus controlos de acesso, causar prejuízo ao seu utilizador ou ao sistema informático infetado, monitorizar a sua atividade ou apropriar-se, corromper, eliminar e/ou alterar dados informáticos.

Em matéria de utilização deste tipo de *software* no âmbito de investigações criminais em ambiente digital, a doutrina costuma referir-se somente aos chamados cavalos de Tróia (*Trojan horses* ou, simplesmente, *Trojans*)[14]. Porém, os cavalos de Tróia representam apenas um dos muitos tipos de *malware* aptos a serem utilizados no âmbito de investigações criminais em ambiente digital, a par, entre outros, das *logic bombs*, do *spyware*, dos *rootkits*, dos vírus, dos *worms*[15] ou mesmo das cada vez mais comuns *blended threats*[16] (ameaças mistas), que incluem mais do que um tipo de *malware*.

Começando pelo conceito mais utilizado, os cavalos de Tróia, podemos procurar defini-los como um tipo de *malware* que se apresenta como sendo inofensivo e induz o visado a empreender numa conduta ativa que resultará na sua instalação no sistema informático visado[17], designadamente fazendo um

13 Em língua original: "*a simple or self-replicating program, which discreetly installs itself in a data processing system, without users knowledge or consent, with a view to either endangering data confidentiality, data integrity and system availability or making sure that users to be framed for computer crime*." – Filiol, 2005: 83.

14 Assim, Albuquerque, 2011: 502.

15 Os vírus e os *worms* fazem parte da categoria do *malware* auto-replicativo, uma vez que conseguem efetuar cópias de si próprios destinadas a serem disseminadas – cf. Filiol, 2005: 88. A esta categoria opõe-se a do *malware* simples a que Adleman chamava de *Epeian viruses*, inspirado na figura de Epeu, da Odisseia de Homero, que construíra o cavalo de Tróia – cf. Adleman, 1988: 361.

16 Como exemplo de *blended threat*, existe o chamado *spy-phishing*, uma forma de ataque de *phishing* que utiliza outras aplicações maliciosas, como sejam cavalos de Tróia ou *spyware*, para obter informação confidencial – cf. Urbas & Choo, 2008: 5.

17 Esta *sedução* para a instalação é muitas vezes gerada por formas de engenharia social em que o que se explora, verdadeiramente, são "*vulnerabilidades nos seres humanos, que também fazem parte do sistema em sentido mais amplo*" – cf. Correia & Sousa, 2010: 16. Neste caso são os próprios utilizadores que ativam, inadvertidamente, as funcionalidades nocivas do *malware*¸ pensando que estão a executar um ficheiro ou a aceder a um *website* inofensivo.

*download* de um anexo de uma mensagem de correio eletrónico[18] ou abrindo uma página *web* infetada com código malicioso (por exemplo, no caso dos chamados *drive-by downloads*[19]). Muitas vezes os cavalos de Tróia são utilizados para criar *backdoors* no sistema informático infetado, isto é, formas escondidas de aceder remotamente ao sistema, contornando os mecanismos de autenticação existentes[20]. Através do acesso propiciado pelo cavalo de Tróia, o terceiro pode recolher informação, como sejam credenciais de acesso a páginas reservadas (como *webmails,* blogues ou perfis em redes sociais), pode instalar mais *malware* (como *spyware*, *keyloggers*[21], vírus ou *worms*[22]), monitorizar a atividade do utilizador no sistema informático infetado, ou mesmo servir como meio para o atacante navegar na Internet de forma anónima, enviando informação a partir do computador infetado.

As *logic bombs*, por seu turno, são uma forma de *malware* não replicativo que se instala num sistema informático e aguarda um incidente ou um evento que funcione como mecanismo de desencadeamento (um *gatilho*) para desempenhar uma função nociva ou ofensiva no sistema informático infetado. Um dos exemplos avançados por Eric Filiol é o do administrador de rede de uma empresa que instala uma *logic bomb* no sistema informático da mesma, programada para verificar diariamente se o seu nome ainda se encontra no registo da contabilidade. A partir do momento em que o seu nome seja eliminado – ou seja, quando o administrador deixar de trabalhar na referida empresa –,

18 A este respeito, afirma Osvaldo Santos o seguinte: "*Os cavalos de Tróia não precisam de usar artifícios técnicos para se disseminarem, pois são os próprios utilizadores que os instalam de livre vontade. Assim, a capacidade de replicação de um cavalo de Tróia depende, acima de tudo, da sua habilidade para seduzir os utilizadores. Esta sedução é feita através dos seus alegados efeitos úteis, que leva muitas vezes os utilizadores a, num gesto de boa vontade, partilhar a aplicação com os seus colegas, amigos e contactos*" – Santos, 2011: 39.

19 V. *infra.*

20 Por exemplo, o cavalo de Tróia *Back Orifice 2000*, geralmente disseminado como anexo em mensagens de correio eletrónico, permitia ao *hacker* recolher informação sobre o computador infetado, executar comandos no sistema, redirecionar tráfego da internet e reconfigurar o sistema informático infetado – cf. Sinrod & Reilly, 2000: 44.

21 O nome *keylogger* advém da contração dos vocábulos *keystroke* e *logging* (o que, em tradução livre, significa registo de teclas premidas) e consiste num *software* que grava e envia informação acerca das teclas premidas pelo utilizador de um sistema informático, com vista à monitorização e documentação da atividade aí empreendida, bem como à obtenção das palavras passe e outras informações relevantes que tenham sido introduzidas através do teclado.

22 Landau, 2010: 54.

a *logic bomb* ativa-se e cifra[23] todos os documentos da empresa, incluindo os *back-ups*, com uma chave secreta[24], tornando-os potencialmente indecifráveis.

Já o *spyware* consiste num tipo de *software* (ou *malware*, consoante o seu propósito[25]) definido genericamente como um programa informático que recolhe informação sobre uma pessoa ou organização sem o seu conhecimento ou consentimento[26]. O *spyware*, por vezes instalado com o auxílio de cavalos de Tróia, pode incluir *sniffers*, que permitem intercetar os pacotes de dados que fluem por aquele ponto da rede, *keyloggers*, que, como se referiu, permitem gravar informação sobre as teclas premidas pelo utilizador[27], bem como instruções para a instalação de um vírus no sistema informático infetado. Adicionalmente, o *spyware* pode incluir a possibilidade de atualização a partir do sistema informático, assim permitindo, simultaneamente, acrescentar novas funções ao programa já instalado, e evitar a deteção por via da atualização de programas de *anti-spyware*[28].

Os *rootkits*, por sua vez, permitem a um intruso ganhar acesso privilegiado de administrador a um sistema informático, geralmente através da exploração de uma vulnerabilidade do sistema operativo ou da descoberta de uma palavra-passe, e costumam ser utilizados para esconder outro tipo de *malware*, como *spyware* ou cavalos de Tróia, tornando-os invisíveis a *anti-vírus* ou *anti-spyware*[29].

Por fim, o vírus é um tipo de *malware* desenhado para se espalhar autonomamente de computador em computador, possivelmente danificando o sistema, corrompendo ou eliminando dados, utilizando a memória disponível no sistema, alterando dados ou instalando outro tipo de *malware*[30], geralmente

---

23 *"Uma cifra é uma técnica concreta de criptografia, isto é, uma forma específica de ocultar informação. Assim, uma cifra transforma um texto em claro num texto cifrado ou criptograma"*, Zúquete: 2013, 26.

24 Filiol, 2005: 99.

25 Muitas vezes o *spyware* é simplesmente utilizado para fins publicitários, nomeadamente recolhendo informação sobre *websites* visitados pelo utilizador do sistema infetado para direcionar a publicidade de acordo com o seu histórico de visitas.

26 Erbschloe, 2005: 25-26.

27 Cf. Clough, 2010: 36.

28 Boldt, 2010: 75.

29 Bickford *et al*.: 2010: 49, e ainda McAfee, 2006: 3-4.

30 Designadamente cavalos de Tróia – cf. Weber & Heinrich: 2012, 14.

integrando-se em código executável[31] que, quando executado, lhe permite ativar-se e infetar mais código[32]. Já os *worms* são em muito semelhantes aos vírus[33], com a diferença de que não precisam de um programa hóspede ou de interação humana para se propagarem, uma vez que constituem um *software* autónomo[34] que se propaga através da Internet[35] e, em algumas modalidades, através das redes GSM/GPRS/UMTS e Bluetooth[36].

Estes são, a nosso ver, os conceitos que apresentam maior relevo para o objeto do presente estudo, uma vez que representam os tipos de *malware* que, quer autonomamente, quer de forma combinada, podem mais facilmente (e com maior utilidade) ser utilizados no contexto de investigações criminais em ambiente digital.

## 2. Processo de instalação e funcionamento

Como tivemos ocasião de indicar *supra*, são vários os modos como o *malware* pode ser instalado num sistema informático. No presente segmento abordaremos os três principais modelos de infeção, a saber: a infeção via suporte físico removível, a infeção via *web browser* e a infeção via *download* voluntário.

Antes do advento da Internet, o modelo de infeção via suporte físico removível, geralmente associado a *malware* auto-replicativo (como vírus e *worms*), era o mais comum. À falta de outro modo de propagação, o *malware* espalhava-se com recurso a disquetes, CDs ou outros suportes destinados a serem fisicamente conectados a sistemas informáticos. Esta modalidade de propagação, embora comparativamente com menor expressividade, perdura nos dias de hoje e pode inclusivamente ser uma arma poderosa para infetar redes locais (as chamadas *Local Area Networks* ou LAN) ou sistemas informáticos desconectados da Internet, como sucedeu nos já referidos casos do *Stuxnet*

31 Daí que Susan Landau se lhe refira como *"fragmento de programa"*, uma vez que necessita de ser inserido noutros programas para poder funcionar (contrariamente aos *worms*) – cf. Landau, 2010: 53.

32 Aycock, 2006: 14.

33 Acerca da multiplicidade de classificações de vírus e *worms* e da difícil tarefa que muitas vezes representa distingui-los, cf. Filiol, 2005: 122 e ss.

34 Uma das formas preferidas para a propagação de *worms* é a utilização de aplicações de correio eletrónico para se autoenviar a todos os contactos do utilizador – cf. Santos, 2011: 38.

35 Aycock, 2006: 15.

36 Correia & Sousa, 2010: 17.

e do *Flame*[37]. Este modelo revela-se de particular utilidade no que respeita à instalação de *malware* para fins de investigação criminal, uma vez que permite que a entidade que o envia se assegure de que apenas infeta o sistema informático específico visado, e não uma multiplicidade indeterminada de sistemas. Assim, o acesso físico ao sistema em causa, ou a promoção da utilização de um suporte físico removível nesse mesmo sistema, tem vantagens óbvias no sentido da instalação do *malware* no sistema certo[38].

O segundo modelo *supra* identificado ocorre nos chamados *drive-by downloads*, em que um utilizador, pensando estar a abrir uma página *Web* inofensiva[39], acede a uma página composta parcialmente por código malicioso (o que pode ocorrer, quer a página tenha sido propositadamente criada para o efeito, quer tenha sofrido uma injeção desse código em virtude da existência prévia de vulnerabilidades de segurança) que deteta vulnerabilidades ou configurações deficientes[40] no sistema informático utilizado para lhe aceder[41] e o infeta com *malware*. Outra vertente deste modelo inclui o *download* automático de *malware* quando o utilizador tenta *clicar* num determinado *link*, geralmente de cariz publicitário (no chamado *malvertising*).

As potencialidades deste modelo para fins de investigação criminal foram, uma vez mais, evidenciadas pelo FBI em agosto de 2013, através da implantação de uma forma de *malware* designada de *Magneto* nos servidores do *Freedom Hosting*, um fornecedor de serviços de armazenamento que continha vários *hidden services*[42] dedicados à pornografia infantil. O *malware* instalado explorava uma vulnerabilidade na versão 17 do *browser Firefox* e permitia identificar a morada MAC[43] e o nome de utilizador do administrador do *Windows*

37 Embora o *Flame* também funcionasse via Bluetooth – Gradigo *et al*., 2013: 37.

38 Assim, Gercke, 2012: 264.

39 Pode até dar-se o caso de o utilizador estar, efetivamente, a tentar aceder a uma página inofensiva, mas em relação à qual tenham sido utilizadas técnicas de redireccionamento que reencaminham a tentativa de acesso para uma página com *malware* – cf. Davis, Bodmer & Lemasters: 2010, 54-55.

40 Cf. Casey, 2011: 377.

41 Landau, 2010: 54 e Aycock, 2006*:* 17.

42 *Hidden services* são *websites* acessíveis apenas através do programa Tor (*The Onion Router*) cujo local de armazenamento é potencialmente indetetável e cujo acesso muito dificilmente permite a identificação dos seus utilizadores – sobre o Freedom Hosting e a chamada *Dark Web*, cf. Ramalho, 2014.

43 *"The Media Access Control (MAC) addresses [...] are part of the data-link layer and can be used to identify a specific computer on a network. These addresses are more identifying than network layer addresses (e.g., IP addresses) because they are generally associated with hardware inside the computer (IP addresses can be reassigned to different computers)."* – Casey, 2011: 624.

que acedia aos referidos *hidden services*, para subsequentemente descobrir o seu verdadeiro endereço IP[44].

Por fim, no último dos modelos que cumpre apreciar, o *malware* pode ser instalado num sistema informático através do *download* de certos ficheiros, quer através da abertura de certos anexos em mensagens de correio eletrónico, quer por via do *download* de programas executáveis (geralmente pirateados ou gratuitos e obtidos através de programas de *peer-to-peer*[45]) quer, ainda, através de falsas atualizações de *software* legítimo (foi esta a opção escolhida pela polícia alemã para instalar o *malware* apodado de *Bundestrojaner* a que aludiremos adiante).

Uma vez instalado no sistema informático visado, o *malware* pode empreender um conjunto de medidas que lhe permitam permanecer indetetável, como sejam promover a sua execução sob um nome aparentemente inofensivo, procurar as tarefas em curso no sistema de modo a poder desativar tarefas comummente associadas a programas de *antivirus*[46], ou ainda substituir-se a um programa normalmente em execução, de modo a que, após consulta dos programas abertos, o utilizador não suspeite da execução de *malware* (uma técnica chamada de *Process Replacement*[47]), pois apenas consegue ver em execução vários programas tidos como confiáveis.

A execução do *malware*, geralmente no caso dos cavalos de Tróia, pode incluir uma comunicação a uma entidade controladora externa com vista à obtenção de instruções futuras ou ao envio de *malware* suplementar. Dependendo dos comandos enviados ou do *malware* a ser instalado, o controlador remoto pode registar as teclas premidas pelo utilizador (com recurso aos já referidos *keyloggers*), vigiar a sua atividade em tempo real, escutar as suas conversas via *Skype* ou outro sistema de *Voice-over-IP* (VoIP) ou mesmo ativar a *webcam* ou o microfone[48] do sistema informático infetado.

---

44 Poulsen, 2013.

45 Os programas de *peer-to-peer* consistem, basicamente, num *software* a ser instalado por cada utilizador no seu computador que permite a troca de ficheiros diretamente entre os computadores dos utilizadores privados, sem recurso a servidores centrais. Para uma explicação detalhada do conceito e origens dos sistemas *peer-to-peer* cf. Vieira, 2009: 421-467.

46 Cf. Aquilina, Casey & Malin, 2008: 492.

47 Cf. Sikorski & Honig, 2012: 257.

48 Cf. Gercke, 2012: 64.

## 3. O *malware* como resposta às medidas antiforenses

Em parte devido à evolução da Ciência Forense Digital e em parte devido à recrudescente intromissão estatal no conteúdo das telecomunicações (pense-se no recente caso do programa *PRISM*), têm sido desenvolvidos programas informáticos com o intuito de frustrar a deteção, monitorização, prova ou imputação de uma determinada atividade *online* ao seu autor: as chamadas medidas antiforenses ou contraforenses.

As medidas antiforenses podem ser definidas, nas palavras de Ryan Harris, como "*quaisquer tentativas de comprometer a disponibilidade ou utilidade da prova no processo forense. Comprometer a disponibilidade da prova inclui quaisquer tentativas de evitar que a prova venha a existir, de esconder prova existente ou de manipular a prova no sentido de assegurar que a mesma deixe de estar ao alcance do utilizador. A utilidade pode ser comprometida através da obliteração da própria prova ou da destruição da sua integridade*"[49] (tradução nossa). Mais sinteticamente, na lapidar afirmação de Scott Berinato: "*Make it hard for them to find you and impossible for them to prove they found you*"[50].

Para compreender a funcionalidade das diversas medidas antiforenses existentes, é necessário, antes de mais, compreender qual o objetivo da Ciência Forense Digital e quais as fases que deverá atravessar.

Assim, ensina Giuseppe Vaciago que o objetivo principal daquilo a que chama de *digital forensics* é a recolha de informação armazenada de forma eletrónica que poderá servir de prova em julgamento. Para tal, define o Autor as fases pré-judiciais envolvidas neste processo, a saber:

a) Identificação de aparelhos de armazenamento eletrónicos ou sistemas de alojamento digital de dados que possam trazer informação sobre crime praticado através de sistemas informáticos;
b) Recolha de prova digital, tanto através da interceção de fluxos informacionais em tempo real, como através da realização de uma cópia integral do aparelho de armazenamento que possa conter dados relevantes;
c) Assegurar a cadeia de custódia da prova assim recolhida[51].

49 Cf. Harris, 2006: S45.

50 Cf. Berinato, 2007.

51 Vaciago, 2012: 31-32.

O objetivo das várias medidas antiforenses existentes é, assim, o de frustrar pelo menos uma das fases deste processo. Antes de procedermos à sua análise, cabe, porém, sublinhar, em primeiro lugar, que restringiremos a nossa análise a apenas algumas das medidas existentes e, em segundo lugar, que a nossa opção pela inclusão de uma medida numa das referidas fases não exclui a sua potencialidade para frustrar qualquer outra fase, mas antes significa que a sua principal potencialidade se reserva àquela fase e não às restantes.

Assim, quanto à fase da identificação, surgem, desde logo, os *softwares* de anonimização que visam impedir que o investigador criminal consiga associar uma certa conduta *online* ao seu autor, escondendo a sua origem, como sejam os servidores *proxy* (ou *gateways* aplicacionais) as *mix cascades* ou o *onion routing*.

O servidor *proxy* é "*um dispositivo ou software que atua em nome dos seus clientes relativamente a um determinado serviço. Os clientes fazem os pedidos ao servidor* proxy *e é este que realmente interage com os servidores de destino para obter as respostas aos pedidos efetuados pelos clientes. Quando as respostas chegam ao servidor* proxy*, este devolve-as aos clientes que fizeram os respetivos pedidos*"[52]. O servidor *proxy* – em particular, o servidor *proxy* baseado na *Web* – funciona, portanto, como um intermediário entre o utilizador e a página visada que envia o tráfego da Internet, escondendo o endereço IP do sistema informático inicial[53].

Acontece que os servidores *proxy*, apesar de permitirem ao utilizador permanecer anónimo perante a página visada, não propiciam completo anonimato, uma vez que o próprio servidor *proxy* consegue identificar o sistema informático do utilizador[54]. Por esse motivo, surgiram as *mix cascades* ou *mix networks*, um sistema de *proxies* em cadeia que faz com que o mesmo *proxy* receba comunicações de várias origens diferentes, misturando-as antes de as enviar aleatoriamente para outro sistema *proxy*, repetindo o processo até chegar ao destinatário final[55].

Destaca-se ainda, nesta matéria, em virtude da sua alargada utilização para a prática de ilícitos criminais, o *Tor*, um programa de *Onion Routing* desenvolvido

52 Cf. Santos, 2011: 62.

53 Cf. Graham, Howard & Olson, 2011: 75.

54 Cf. Weber & Heinrich, 2012: 17.

55 Cf. Bettini *et al.,* 2009: 88.

com o objetivo de garantir a confidencialidade e inviolabilidade das comunicações dos seus (ou entre os seus) utilizadores, bem como o anonimato do seu remetente, e que funciona com base no envio da comunicação por um sistema de *roteamento*, passando por diversos pontos distintos sob diferentes camadas de cifragem, até atingir o seu destinatário[56].

Todavia, as medidas antiforenses não atuam só na frustração do objetivo inicial de identificação do sistema informático inicial. Entre algumas das medidas utilizadas para frustrar (principalmente) a atividade da recolha de prova, destacam-se a esteganografia, a cifragem de dados ou a limpeza do disco (*data wiping*).

A esteganografia consiste "*ao nível da informática, em ocultar de forma dissimulada informações em ficheiros eletrónicos quer sejam documentos, imagens ou de outro tipo. Por exemplo, dados podem ser ocultados num ficheiro e imagem através de uma alteração ligeira de um* bit *que compõe conjuntamente com outros um pixel. Alterações deste género, alargados a toda a imagem, podem dissimular dados.* […] *Através de uma chave específica para identificar estes* bits *que foram alterados, pode obter-se a informação que estava dissimulada*"[57]. O recurso a esta técnica permite *esconder* em ficheiros áudio, de imagem ou de vídeo aparentemente inofensivos, outras mensagens, imagens ou conteúdo audiovisual de cariz potencialmente ilegal[58].

Já a cifragem de dados, como tivemos ocasião de referir, permite ao seu utilizador transformar um dado ficheiro num criptograma, o que torna o acesso ao ficheiro decifrado potencialmente impossível para quem não tenha a chave[59].

---

56 Para uma explicação do funcionamento do *Tor*, ainda que tendencialmente orientada para os casos em que os *relays* são geridos por utilizadores da rede *Tor*, Ramalho, 2014: 390-394

57 Santos, Bessa & Pimentel, 2008: 243.

58 A mera deteção deste tipo de ficheiros pode revelar-se problemática. Entre as técnicas utilizadas para descobrir ficheiros nos quais se recorreu a esta tecnologia, encontra-se a análise de ficheiros de imagem com vista à verificação da existência de um histograma incomum (a distribuição de luz numa imagem) ou uma análise estatística dos ficheiros armazenados no sistema visado, em busca de propriedades incomuns, o que poderá ser cumulado com uma pesquisa, no mesmo sistema, de conhecidos programas de esteganografia.

59 No que respeita à cifragem, ensina Giuseppe Vaciago o seguinte: "*É, na realidade, totalmente inútil tentar prever quanto tempo demoraria a desbloquear dados protegidos por palavra-passe uma vez que, dependendo do tipo de chave de encriptação e de* software *de desencriptação utilizado, o tempo envolvido poderia variar entre uns segundos até muitos milhares de anos. Uma palavra-passe de 20-bit, por exemplo, permite um milhão de combinações possíveis, sendo que um computador portátil normal com uma capacidade de processamento de cerca de um milhão de computações por segundo, poderia muito bem descobrir*

Por outro lado, a limpeza do disco consiste na eliminação definitiva dos dados armazenados num determinado sistema informático. Com efeito, o mero ato de enviar um ficheiro para a reciclagem do computador e de esvaziar esta pasta não permite, em geral, a remoção definitiva do ficheiro do sistema informático no qual se encontra. Na verdade, "*quando se apaga um ficheiro isso não quer dizer que se remove o seu conteúdo do disco. É meramente removido o apontador a esse ficheiro. Os dados são armazenados em* clusters*, que são unidades constituídas por um conjunto de* bits. *Pelo facto das partes de um ficheiro não serem sempre armazenadas em* clusters *contíguos de um disco, sem uma ordem aparente e em diferentes localizações, a remoção dos já referidos apontadores faz com que a reconstituição de um ficheiro seja difícil de ser concretizada*"[60]. Daí que uma das medidas antiforenses mais populares seja a utilização de *software* específico para substituir os ficheiros *eliminados* por dados aleatórios ou com os mesmos dados para cada setor do disco, de modo a que os dados iniciais sejam irrecuperáveis. Existem inclusivamente relatos de um *software* intitulado de *Panic Button*, comummente utilizado por consumidores de pornografia infantil na Internet, que efetua um procedimento semelhante ao aqui descrito em caso de suspeita da iminência ou da decorrência de uma investigação policial ao sistema informático no qual os dados se encontram armazenados[61].

Por fim, no que respeita à última das fases *supra* enunciadas, há que destacar os ataques contra perícias forenses. Com efeito, as ferramentas com que se efetuam as perícias forenses e a recolha de prova digital têm como pressuposto que, uma vez instaladas, a recolha de prova não será afetada pela sua presença ou utilização. Contudo, certo *software*, uma vez instalado num sistema informático visado por uma perícia forense, ativa mecanismos de agressão às próprias ferramentas com que se efetuam as perícias, falsificando ou modificando a prova[62] e, consequentemente, perturbando a sua fidedignidade em sede judicial.

---

*a chave de encriptação em menos de um segundo. Contudo, ao mesmo computador demoraria cerca de 2285 anos a desbloquear dados protegidos por uma palavra-passe de 56-bit. Para se ter uma ideia da complexidade da tarefa em termos práticos, temos de considerar o PGP (Pretty Good Privacy), o programa de encriptação mais popular no mercado hoje, que usa uma chave de encriptação de 1024-bit."* (tradução nossa) – cf. Vaciago, 2012: 123.

60 Santos, Bessa & Pimentel, 2008: 240.

61 Informação prestada por Troels Oerting, Diretor do European Cybercrime Centre (EC3), na *I Europol-Interpol Cybercrime Conference* ocorrida na Haia, no passado dia 25 de setembro de 2013.

62 Cf. Kessler, 2007.

Em face da proliferação das medidas antiforenses *supra* referidas e de muitas outras, bem como da facilidade com que as mesmas podem ser adotadas por utilizadores com conhecimentos técnicos medianos, afigura-se como de superior importância, em casos cuja gravidade assim o justifique, a utilização de *malware* instalado sub-repticiamente no computador visado para permitir a recolha de prova[63].

Com efeito, a infeção de sistemas informáticos que se socorram de ferramentas anonimizadoras permitirá obter informação sobre a sua localização e sobre a atividade desenvolvida pelos seus utilizadores. Por outro lado, quando existam ferramentas de esteganografia ou cifragem, a monitorização do sistema informático visado com recurso a *malware* permitirá, simultaneamente, tomar conhecimento da existência desses ficheiros (quando o utilizador a eles recorra) e captar as palavras-passe introduzidas com recurso a *keyloggers*.

A tudo isto acresce o facto de o utilizador comum não ter por hábito proceder a limpezas de disco ou à eliminação ou danificação de suporte probatório importante quando não sabe que está a ser investigado, a menos, é certo, que existam mecanismos técnicos instalados no sistema informático visado que automaticamente empreendam uma dessas atividades, quando detetem a utilização de *software* forense, pelo que haverá que procurar contornar esse risco com a atualização do próprio *malware*.

## CAPÍTULO II – ORIGEM E EVOLUÇÃO DA UTILIZAÇÃO DE *MALWARE* COMO FERRAMENTA DE INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL

### 1. A experiência norte-americana: o *Magic Lantern* e o CIPAV

A experiência norte-americana tem sido particularmente atribulada no que respeita ao uso de *malware*. Desde logo porque tem sido marcada por repetidas revelações, não autorizadas, do uso secreto, por parte das polícias, de diferentes tipos de *malware*, cuja fundamentação jurídica é por vezes encontrada em leituras algo (es)forçadas da Constituição dos Estados Unidos da América. Tendo em atenção que uma análise detalhada desta evolução é incompatível com o carácter sintético que queremos imprimir ao presente segmento, limitar-

63 Pradillo, 2013: 177-178

-nos-emos a oferecer uma breve exposição dos episódios que se nos afiguram como mais relevantes para o nosso estudo[64].

O primeiro caso a merecer atenção mediática generalizada sobre o uso de *keyloggers* por órgãos de polícia criminal data de janeiro de 1999 (ainda que aqui se trate simultaneamente de *malware* e *hardware*), quando, no âmbito de uma investigação criminal conduzida pelo FBI a Nicodemo S. Scarfo – um conhecido membro de uma organização mafiosa suspeito de infrações criminais relacionadas com a gestão de um negócio de jogo ilegal –, se descobriu que este teria armazenado no seu computador ficheiros cifrados que se suspeitava poderem revestir elevado valor probatório[65].

Em face da necessidade de obtenção daqueles ficheiros, e uma vez que os dados cifrados pelo *software* utilizado (o *Pretty Good Privacy*, geralmente designado pela sigla PGP) apenas podiam ser decifrados por quem tivesse a chave, o FBI solicitou novo mandado judicial, desta feita para introduzir um *keylogger*, diretamente no computador do suspeito, capaz de captar a palavra passe do PGP[66] e de a enviar por ondas rádio para o FBI[67]. O mandado judicial foi obtido e o *keylogger* foi instalado fisicamente – neste caso, também sob a forma de *hardware* – algures entre o teclado e o computador do suspeito. Dois meses volvidos[68] e a palavra-passe[69] foi finalmente obtida[70], assim permitindo ao FBI deter o suspeito e decifrar o conteúdo do ficheiro pretendido[71].

---

64 Para um estudo aprofundado do percurso que o problema das escutas e demais mecanismos de interceção de comunicações têm tido nos EUA, v. por todos, Landau, 2010.

65 Os factos encontram-se descritos em maior detalhe em *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001).

66 Cf. Declaração do Agente do FBI que solicitou a emissão do mandado judicial, com a descrição do modo de funcionamento do *keylogger* e demais informações de relevo, disponível em: http://epic.org/crypto/scarfo/murch_aff.pdf [consultado em: 05-10-2013].

67 Cf. Landau, 2010: 133.

68 Cf. Murphy, 2002.

69 A palavra-passe era NDS09813-050, o número de identificação prisional do pai de Nicodemo S. Scarfo – Mohay et al, 2003: 120.

70 Cumpre referir que, para evitar eventuais violações do *Wiretap Act*, este *keylogger* apenas funcionava quando o computador não estava ligado à Internet – cf. Sheetz: 2007, 142.

71 O processo seguiu os seus trâmites, com a apresentação de uma *motion to suppress evidence* por parte do suspeito, a qual foi objeto de uma interessante decisão judicial (em sentido desfavorável), da qual, pelo seu interesse, se cita o seguinte excerto: "*In this day and age, it appears that on a daily basis we are overwhelmed with new and exciting, technologically-advanced gadgetry. Indeed, the amazing capabilities bestowed upon us by science are at times mind-boggling. As a result, we must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise*

As compreensíveis dificuldades práticas suscitadas pela instalação física de *keyloggers* em computadores de suspeitos da prática de atividades criminosas, bem como as crescentes gravidade e internacionalização da criminalidade – o que veio a receber particular atenção após o ataque às Torres Gémeas – tornaram óbvia a necessidade de instalação deste tipo de mecanismos por via remota e sem necessidade de *hardware*.

Assim surgiu, em 2001, o *Magic Lantern*, um *keylogger* que poderia ser instalado sub-reptícia e remotamente via Internet no sistema informático visado – localizado ou não nos EUA – quando este pertencesse a indivíduos suspeitos de estarem relacionados com atividades criminosas, em particular de natureza terrorista. O *Magic Lantern* podia ser instalado, quer através da abertura, no computador visado, de anexos em mensagens de correio eletrónico enviadas para o suspeito, quer por via da exploração de vulnerabilidades nos sistemas operativos instalados no sistema informático em causa[72]. Todavia, uma vez que certos programas anti-vírus conseguiam detetar o *Magic Lantern*, consta que o Governo norte-americano solicitou a algumas empresas dedicadas à sua comercialização que evitassem interferir com o mesmo[73].

O *Magic Lantern* viria a dar lugar ao *Computer and Internet Protocol Address Verifier* (CIPAV)[74], um tipo de *malware* que juntava à lista de informação recolhida, entre outras, o endereço IP e/ou endereço MAC do suspeito e a respectiva localização, bem como a lista de programas em funcionamento num dado momento, o sistema operativo utilizado (tipo, versão e número de série), a conta de utilizador aberta naquele momento (uma vez que um só computador pode ter mais do que uma conta de utilizador) e o último *website* visitado[75].

---

*true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes. Each day, advanced computer technologies and the increased accessibility to the Internet means criminal behavior is becoming more sophisticated and complex. This includes the ability to find new ways to commit old crimes, as well as new crimes beyond the comprehension of courts.*" – disponível em: http://www.leagle.com/decision/2001752180FSupp2d572_1686 [consultada em: 10-10-2013], cf. ainda – cf. Woo & So, 2002: 533. Como se referiu, o facto de os ataques de 11 de setembro terem ocorrido 3 meses antes da prolação da citada decisão não é despiciendo, uma vez que a partir daí começou a existir maior tolerância perante o recurso a estes meios. O caso acabou por ser objecto de um acordo de *plea bargaining*, em 28 de Fevereiro de 2002, o que obstou a que houvesse uma decisão judicial de mérito sobre o mesmo.

72 Curran *et al*., 2008: 309.

73 Woo & So, 2002: 524.

74 Cf. Soghoian, 2010: 400-401.

75 Cf. Landau, 2010: 133.

Embora haja relatos da sua utilização que remontam a 2001 (o que poderia indicar a sua coexistência com o *Magic Lantern*), o CIPAV apenas viria a ser divulgado em 2007, por ocasião da publicitação, pela comunicação social, de um pedido de mandado para a sua utilização, apresentado pelo Agente Especial do FBI Norman Sanders, no âmbito de um processo em que se procurava detetar o autor de várias ameaças de bomba[76].

Foi, porém, apenas em abril de 2011, na sequência de um pedido submetido pela *Electronic Frontier Foundation* ao abrigo do *Freedom of Information Act*[77], que o FBI veio a divulgar vários documentos com informação detalhada sobre a utilização, enquadramento legal e funcionamento do CIPAV[78]. Da consulta dos referidos documentos retiram-se duas conclusões de particular relevância: em primeiro lugar, que este programa era abundantemente utilizado, inclusivamente por entidades governamentais que não o FBI, e, em segundo lugar, que, numa primeira fase, existiam vários entendimentos quanto aos requisitos legais para a sua admissibilidade, os quais encontrariam, num dos pólos, os defensores da desnecessidade de qualquer procedimento legal para a sua utilização e, noutro pólo, os defensores de que a sua utilização dependeria de autorização judicial[79].

Apesar do impacto que a divulgação desta informação viria a ter, o recurso a *malware* no contexto de investigações criminais persiste. Demonstração disso é o facto de, em abril de 2013, ter sido tornada pública uma ordem judicial[80], subscrita pelo Juiz Stephen Smith, da Divisão de Houston do Tribunal de Distrito do Texas, na qual foi negada autorização judicial para a utilização de um tipo de *malware* não identificado

76 Para consultar a digitalização do documento, v. http://www.wired.com/images_blogs/threatlevel/files/timberline_affidavit.pdf, [consultado em 4-10-2013].

77 Título 5 do *United States Code*, § 552, alterado pela Lei n.º 110-175, 121 Stat. 2524, e pela Lei n.º 111-83, § 564, 123 Stat. 2142, 2184.

78 Disponíveis para *download* em https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav [consultado em 10-10-2013].

79 De acordo com a referida documentação, a solução adotada acabou por ser dividida em duas fases: em primeiro lugar seria necessário um mandado judicial para a intrusão no sistema informático visado e, em segundo lugar, seria necessária uma *Pen/Trap order* para autorizar a vigilância – cf. p. 169 da documentação facultada pelo FBI, disponível em: https://www.eff.org/files/FBI_CIPAV-08-p169.pdf [consultado em 10-10-2013].

80 Decisão disponível em: http://pt.scribd.com/doc/137842124/Texas-Order-Denying-Warrant [consultada em: 10-10-2013].

no âmbito de uma investigação criminal[81], com o principal fundamento que o seu processo de instalação não se encontrava devidamente especificado e, consequentemente, existiria incerteza quanto à possibilidade de o *malware* em causa ser instalado em sistemas informáticos que não o visado.

Não obstante não conste da decisão o nome do *malware* em causa, a verdade é que, caso se trate do CIPAV, será uma versão mais avançada do que aquela explicada nos documentos cedidos pelo FBI, uma vez que acrescenta às funções *supra* descritas as seguintes: registos da atividade na Internet, incluindo registos da *firewall*, *caches*, histórico do *browser*, *cookies*, páginas selecionadas como favoritas, termos de pesquisa utilizados em motores de busca, registos de endereços URL introduzidos manualmente pelo utilizador, nomes de utilizador e palavras-passe gravadas, contactos e conteúdos de correio eletrónico, registos de *chat* e outros programas de *messaging*, bem como fotografias contidas no sistema informático visado, entre outros dados. Mais, o *malware* em causa permitia ainda controlar remotamente o sistema informático visado e tirar fotografias com recurso à *webcam* instalada no mesmo, assim permitindo a identificação do seu utilizador, bem como do local em que se encontrava.

## 2. A experiência alemã: vicissitudes do *Bundestrojaner*

Em 2006, no âmbito de uma investigação criminal sobre factos relacionados com terrorismo, um Procurador da República apresentou um pedido de mandado judicial para efetuar uma pesquisa remota ao computador de um suspeito, através da instalação de um cavalo de Tróia.

O pedido foi rejeitado em 25 de novembro de 2006 e o mesmo Procurador interpôs recurso para o Tribunal de Justiça Federal da Alemanha (*Bundesgerichtshof*), tendo para o efeito alegado que as disposições legais constantes do Código de Processo Penal alemão referentes à busca em locais físicos, à pesquisa e apreensão de documentos e de sistemas informáticos de armazenamento e à apreensão e conservação de prova, permitiriam a utilização daquele meio de obtenção de prova, porquanto se estaria perante uma medida processual substancialmente análoga à busca em locais físicos[82].

---

81 Embora o Tribunal, na nota de rodapé n.º 10, faça uma referência ao CIPAV, afigura-se que a mesma reveste cariz meramente exemplificativo, deixando em aberto a possibilidade de estar, ou não, em causa uma versão mais avançada do CIPAV.

82 Vaciago, 2012: 125.

O Tribunal viria a decidir em sentido inverso, por entender, em traços gerais, que a analogia entre a busca em locais físicos e as ditas *buscas* em computadores improcedia e, consequentemente, que inexistia supedâneo legal expresso que permitisse conceder o mandado requerido[83].

Menos de um mês volvido sobre a dita decisão, no dia 20 de dezembro de 2006, a Lei de Proteção da Constituição da Renânia do Norte-Vestefália foi alterada, tendo sido introduzida no seu § 5.2(11)[84] uma norma que conferiu à entidade responsável pela proteção da Constituição (*Bundesamt für Verfassungsschutz*) o poder de aplicar medidas de obtenção de informação traduzidas na monitorização secreta acompanhada de outras atividades de reconhecimento na Internet, como a participação encoberta em *chats* e ainda – embora esta solução seja menos clara – o acesso a *webmails* e ainda o acesso *websites* de acesso restrito com recurso a credenciais recolhidas de diversas fontes, como sejam informadores[85]. Por fim, e para o que aqui releva, a lei em causa permitia ainda o acesso secreto a sistemas informáticos, com recurso à exploração de vulnerabilidades técnicas, para a instalação de *malware*[86] que permitisse à referida autoridade espiar, monitorizar, analisar o conteúdo e até controlar o sistema informático afetado embora, naturalmente, a aplicabilidade desta norma estivesse limitada às funções da autoridade para proteção da Constituição, previstas no §3 da Lei de Proteção da Constituição, designadamente a recolha e análise de informação a casos relativas a atividades ilícitas que ameaçassem a livre ordem democrática fundamental

83 BGH StB 18/06.

84 A norma dita o seguinte: "*(2) De acordo com* § 7, a autoridade para proteção da Constituição pode aplicar as seguintes medidas para adquirir informação como meio de serviço de *intelligence*:
[...] *11. monitorização secreta e outro reconhecimento da Internet, como em particular participação encoberta nos seus meios de comunicação e de pesquisa, bem como acesso secreto a sistemas informáticos envolvendo a instalação de meios técnicos. Na medida em que tais medidas constituam uma ingerência no segredo da correspondência, correio ou telecomunicações ou seja equivalente a tal ingerência em termos de natureza e gravidade, esta será apenas admissível sob as condições do artigo 10 da Lei Fundamental*".

85 Assim, Abel & Schafer, 2009: 107-110.

86 O Tribunal Constitucional alemão, no acórdão que se citará de seguida, referiu expressamente que "*tais medidas já foram executadas em casos isolados por autoridades federais sem base legal. Pouco se sabe da natureza da execução prática de* 'buscas online' *prévias ou dos seus sucessos*". A utilização prévia deste tipo de *malware* em processos de natureza criminal é inclusivamente indiciada pelo teor dos *supra* referidos documentos facultados pelo FBI a propósito do CIPAV, nos quais consta que, no dia 24 de julho de 2007, foi enviada uma mensagem de correio eletrónico, proveniente de um remetente cuja identidade foi omitida, na qual se referia a existência de interesse, por parte *dos alemães*, em obter mais informações sobre o CIPAV – cf: https://www.eff.org/files/FBI_CIPAV-08-p9.pdf [consultado em 13-10-2013].

ou a continuada existência ou segurança da Federação ou de uma *Land* ou respetivos membros[87].

Pouco tardou para que o Tribunal Constitucional Federal fosse chamado a pronunciar-se quanto à conformidade constitucional da norma em causa e ainda do recurso a este tipo de meio de obtenção de prova, o que viria a suceder em 27 de fevereiro de 2008[88].

O Tribunal começou por analisar o problema à luz de três direitos fundamentais: (i) o direito à privacidade da correspondência, do correio e das telecomunicações, (ii) o direito à inviolabilidade do lar e (iii) o direito à autodeterminação informacional. Todavia, a especificidade do meio de obtenção de prova em causa reclamava uma tutela constitucional que extravasava o objeto de cada um dos referidos direitos fundamentais. Assim, em face da necessidade de oferecer, de forma mais abrangente, proteção constitucional à integridade do sistema informático do visado, bem como aos dados armazenados e transmitidos com recurso ao mesmo, o Tribunal cunhou o direito fundamental à confidencialidade e integridade de sistemas informáticos[89] (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). O direito fundamental assim formulado, fundado na dignidade da pessoa humana e no direito ao livre desenvolvimento da personalidade, protegeria, em suma, "*o interesse do utilizador em assegurar que os dados criados, processados e armazenados pelo sistema informático coberto pelo seu âmbito de proteção, permaneçam, confidenciais*"[90].

Submetida a norma em análise ao crivo constitucional, o Tribunal Constitucional Federal concluiu que a mesma violava ainda os princípios da clareza e certeza legal e da proporcionalidade, pelo que, na referida data, veio a concluir pela sua inconstitucionalidade. Fê-lo, contudo, oferecendo as

87 Embora a lógica subjacente fosse a da prevenção do terrorismo, a verdade é que, como bem realça o Tribunal Constitucional alemão, "*a área de aplicação da revisão não se restringe ao combate ao terrorismo, quer de forma explícita, quer como consequência do seu contexto sistemático. A norma requer uma justificação para toda a sua área de aplicação*".

88 Cf. Acórdão BverfG, 1 BvR 370, 595/07, de 27 de fevereiro de 2008, disponível em: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html [consultado em 14-10-2013].

89 Há que referir, porém, que já em 2006, González-Cuellar Serrano sustentava entendimento semelhante ao defender a existência de um direito à não intromissão no ambiente digital (*derecho a la no intromisión en el entorno digital*), enquanto decorrência do chamado direito à liberdade informática – Serrano, 2006: 916.

90 Embora com a ressalva de que que "*a expectativa de confidencialidade e integridade a ser reconhecida pela perspetiva dos direitos fundamentais apenas existe na medida em que a pessoa em causa use o sistema informático como seu e assim possa presumir, de acordo com as circunstâncias, que ele ou ela, por si só ou juntamente com outros autorizados a utilizá-lo, disponham do sistema informático de modo autodeterminado*".

coordenadas para uma futura formulação legal do mesmo meio de obtenção de prova, em conformidade com os imperativos constitucionais violados.[91]

Assim, através da Lei para a defesa face aos perigos do terrorismo internacional através do Bundeskriminalamt (*Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*), de 25 de dezembro de 2008, foi introduzida no ordenamento jurídico alemão a possibilidade, a título excecional, de recurso a *malware* para efeitos de prevenção de crimes de terrorismo[92].

Fora, então, estabelecida a necessidade de precedência de lei para a utilização de *malware*, e formulada a respetiva norma no seguimento das orientações do Tribunal Constitucional.

Acontece que, no dia 8 de outubro de 2011, foi divulgada (com impacto significativo na comunicação social), por uma associação de *hackers* autointitulada de *Chaos Computer Club* (CCC), a utilização, por parte de órgãos de polícia criminal alemães, de um tipo de *malware* – comummente qualificado como um cavalo de Tróia mas aparentemente uma *blended threat* – que viria a ficar conhecido como o *Bundestrojaner* ou o *Staatstrojaner*.

Este tipo de *malware*, entretanto vendido também à Áustria, consiste numa espécie de *malware* enviado para o computador do suspeito sob a forma de uma comum atualização de *software* e que, após instalação, permite monitorizar toda a atividade do visado na Internet, incluindo gravar as chamadas *VoIP* (por exemplo, via *Skype*), bem como captar palavras-passe, introduzir dados no sistema informático visado e, inclusivamente, ativar o seu *hardware*, utilizando o microfone e a *webcam* para gravar sons e tirar fotos que subsequentemente serão enviadas para as entidades que conduzem a investigação[93].

Apesar do entendimento exposto pelo Tribunal Constitucional Federal, e do carácter excecional – e necessariamente assente em previsão legal expressa e específica quanto à instalação e possibilidade de utilização, ainda que sem interceção de telecomunicações, do *malware* – que este meio de obtenção de prova à partida deveria revestir, há notícias de que o *Bundestrojaner* foi utilizado mais de cinquenta vezes, sem que a sua instalação se tenha limitado a casos de terrorismo[94].

---

91 Para uma descrição detalhada do entendimento do Tribunal, v., Abel & Schafer, 2009 e Pradillo, 2013: 181-185.

92 Cf. Pradillo, 2009: 5 e Rogall, 2009: 120-121

93 Para uma análise mais detalhada da origem e funcionamento do *Bundestrojaner* e da utilização deste tipo de programas pela Suíça e pela Áustria, cf. Weber & Heinrich, 2012: 60-65.

94 Cf. Rosenbach, 2011.

## 3. O regime espanhol vigente e o *Projecto Gallardón*

Em Espanha inexiste, atualmente, legislação específica sobre o uso de *malware* como meio de obtenção de prova em processo penal. Tal facto, porém, não torna a sua inadmissibilidade pacífica na doutrina[95] e tão-pouco permite concluir que este meio não venha a ser criado por via de uma extensão jurisprudencial de disposições processuais existentes.

A propósito desta *legitimação* jurisprudencial de meios de obtenção de prova atípicos, e a título exemplificativo, Ortiz Pradillo dá-nos conta da consagração, por meio de três acórdãos do Supremo Tribunal Espanhol[96], da utilização de dispositivos eletrónicos designados de *IMSI Catchers* ou *Cell Site Simulators* destinados a obter, a partir da localização física de determinados telemóveis e da sua proximidade das antenas que lhes proporcionam a rede telefónica, não só a sua localização física aproximada, mas também o seu número IMSI (*International Mobile Subscriber Identity*) e, com base no mesmo, o número de telemóvel que se lhe encontra associado.

A admissibilidade da utilização destes dispositivos no ordenamento jurídico espanhol foi encontrada pelo Supremo Tribunal no regime que regula a recolha e tratamento, para fins policiais, de dados pessoais por forças e corpos de segurança (artigo 22.º da Lei Orgânica 15/1999, de 13 de dezembro, sobre a proteção de dados pessoais), o qual, como bem nota o Autor, não prevê a necessidade de precedência de mandado judicial para a sua aplicação. Confrontado o regime do artigo 22.º da Lei Orgânica 15/1999, jurisprudencialmente aplicado à recolha destes dados – que o Tribunal qualificou como dados pessoais –, e aquele constante do regime que regula a petição de cessão dos mesmos dados às operadoras telefónicas (Lei n.º 25/2007, de 18 de outubro, sobre a conservação de dados relativos a comunicações eletrónicas e às redes públicas de comunicações), no qual se prevê a necessidade de precedência de mandado judicial, constata-se que a decorrência do entendimento do Tribunal é que a autorização judicial

95 Velasco Nuñez, por exemplo, embora reconheça as dificuldades suscitadas pela ausência de suporte legal, admite *de jure condito* o recurso a estes meios com base na aplicação analógica do regime das interceções de comunicações electrónicas ou magnéticas, à luz da jurisprudência do Supremo Tribunal e do Tribunal Constitucional de Espanha sobre ingerências sobre o direito ao segredo das telecomunicações – Nuñez, 2010: 136-137 e 2011: 24. Já Mercedes Fernández López limita-se a condicionar a aplicabilidade destes meios a critérios de imprescindibilidade, proporcionalidade e gravidade do crime em causa, devendo a mesma ser precedida de despacho judicial. A Autora veda, porém, a utilização do *malware* nos casos em que a mesma tenha finalidade preventiva ou em que o sistema informático se encontre localizado no estrangeiro, cf. López, 2011: 281-282.

96 O primeiro de 20 de maio de 2008 (RJ 2008/4387), o segundo de 18 de novembro de 2008 (RJ 2009/2089) e o terceiro de 28 de janeiro de 2009 (RJ 2009/3299).

não será exigível quando os órgãos de polícia criminal possam *motu próprio*, obter estes dados, mas será legalmente imposta quando os mesmos órgãos precisem de cooperação das operadoras telefónicas para os obter[97].

Realçando a disparidade injustificada de requisitos nesta matéria, Ortiz Pradillo adverte que o entendimento jurisprudencial segundo o qual a recolha destes dados "*no contexto de uma investigação criminal – nunca com carácter exclusivamente exploratório – para a descoberta de um crime particularmente grave pode ser considerada proporcional, necessária e, como tal, livre de qualquer violação de direitos e liberdades fundamentais*", poderá abrir caminho a que, do mesmo modo, se procure obter *dados pessoais* em redes Wi-Fi abertas, com recurso a '*spyware*'".

Crítico desta tendência da jurisprudência em se substituir ao legislador, e manifestando a sua oposição a uma interpretação que procure legitimar o uso de *malware* nos meios de obtenção de prova existentes na *Ley de Enjuiciamento Criminal* (LEC), o Autor reconhece, porém, que é possível que a jurisprudência espanhola venha, à semelhança dos casos referidos, a interpretar certas normas no sentido de fundamentarem a admissibilidade da utilização de *malware*, em violação "*das exigências mínimas de legalidade e clareza estabelecidas pelo TEDH*"[98].

Sustentava o Autor que, caso tal viesse a suceder em vez da desejada reforma da LEC, sempre deveriam ser jurisprudencialmente fixados certos requisitos para a utilização de *malware* que incluíssem, designadamente, a obrigatoriedade de precedência de mandado judicial[99] (i); a imposição do carácter secreto da aplicação da medida (ii); o estabelecimento de uma obrigatoriedade de cooperação de terceiros, designadamente das operadoras de telecomunicações,

97 Pradillo, 2012: 187-191 e 2013: 188-191.

98 Pradillo, 2012: 198.

99 Cabe, porém, referir aqui que, mesmo se se admitisse a aplicação, no plano do direito constituído, deste meio de obtenção de prova, sempre se nos afiguraria como imperativa a precedência de mandado judicial para a sua utilização, em particular face ao entendimento propugnado pelo Supremo Tribunal espanhol no seu aresto de 17 de abril de 2013 (Sentencia 342/2013), do qual se transcreve o seguinte excerto: "*el ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y a la protección de datos personales susceptibles de protección constitucional en el ámbito al derecho a la intimidad y la protección de datos (art. 18.4 de la CE (LA LEY 2500/1978)). Pero su contenido también puede albergar – de hecho, normalmente albergará – información esencialmente ligada a la inviolabilidad de las comunicaciones* [...] *En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía, ha de contar con el presupuesto habilitante de una autorización judicial*".

quando tal seja necessário (iii); o dever de fundamentação da decisão judicial (iv); a excecionalidade da medida e respetiva aplicação somente a crimes particularmente graves (v); e ainda a recolha de modo a assegurar a autenticidade e a integridade da informação obtida (vi).

Acontece, porém, que a via seguida no ordenamento jurídico espanhol parece ter sido outra. Assim, encontra-se atualmente em discussão uma profunda reforma ao nível processual espanhol, que previsivelmente se traduzirá na aprovação de um novo Código de Processo Penal, realizada através do denominado (ante)projeto *Gallardón*[100], em cujo artigo 350.º se prevê, mediante prévia autorização judicial, "*a utilização de dados de identificação e códigos, assim como a instalação de um software, que permitam, de forma remota e telemática, o exame à distância e sem conhecimento do seu titular ou do utilizador do conteúdo de um computador, dispositivo eletrónico, sistema informático, instrumento de armazenamento em massa de dados informáticos ou base de dados, sempre que a medida resulte proporcionada para a investigação de um delito de especial gravidade e seja ademais idónea e necessária para o esclarecimento do facto investigado, a averiguação do seu autor ou a localização do seu paradeiro*".

O regime previsto no novo Título XI, subordinado à epígrafe "*registros remotos sobre equipos informáticos*" aparenta cumprir a generalidade dos requisitos propostos por Ortiz Pradillo, prevendo, inclusivamente, um – a nosso ver indispensável – dever de fundamentação, por parte do juiz, sobre a idoneidade, necessidade e proporcionalidade da medida (art. 350.º, n.º 2, do Anteprojeto), bem como a especificação dos computadores, dispositivos eletrónicos, sistemas informáticos ou parte dos mesmos, meios de armazenamento de dados informáticos ou bases de dados e dados informáticos objeto da medida (alínea *a)*); o alcance da medida, a forma com que se procederá ao acesso e apreensão dos dados ou arquivos informáticos relevantes para a causa e o *software* mediante o qual se executará o controlo de informação (alínea *b)*); os agentes autorizados para a execução da medida (alínea *d)*); a autorização, caso se aplique, para a realização e conservação de cópias dos dados informáticos (alínea *e)*); as medidas necessárias para a preservação da integridade dos dados armazenados, assim como para a inacessibilidade ou supressão dos mesmos do sistema informático a que tenha tido acesso (alínea *f)*). No artigo 351.º prevê-se ainda

100 O nome comummente atribuído a este Projeto advém do facto de ter sido proposto pelo Ministro da Justiça espanhol Alberto Ruiz Gallardón.

o dever de colaboração, entre outros, dos provedores de serviços de acesso e dos responsáveis pelo sistema informático ou base de dados objeto de registo.

Sem prejuízo de a técnica legislativa poder dar azo a uma margem de densificação porventura excessiva ao juiz de instrução, designadamente por pecar pela ausência de definição do conceito de "*delitos de especial gravidad*"[101], na eventualidade de ser aprovada a proposta em causa, o ordenamento jurídico espanhol ganhará em termos de clareza e segurança quando aplicar este tipo de medidas.

## 4. A propensão para a consagração do *malware* como meio de obtenção de prova em ambiente digital: o Projeto HIPCAR e a Diretiva 2011/92/EU do Parlamento Europeu e do Conselho, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil

Com o aperfeiçoamento das técnicas utilizadas para a prática do cibercrime à escala global, tem crescido o interesse na criação de instrumentos uniformes a nível internacional para o combate a esta nova criminalidade. Com efeito, considerando que o Estado no qual o visado atua pode não ser o Estado no qual o resultado típico se produz, e uma vez que a aplicação destes instrumentos continua, pelo menos tendencialmente, limitada pelo princípio da territorialidade da aplicação da lei processual penal, existe todo o interesse em que os instrumentos tidos como mais eficazes se encontrem consagrados no maior número possível de Estados.

Daí que, em particular desde a Convenção sobre o Cibercrime, de 23 de novembro de 2001, se tenha assistido ao surgimento – ainda que tímido – de iniciativas de cariz supranacional que visam promover a adoção do recurso ao *malware* como meio de obtenção de prova em ambiente digital. Assim, em dezembro de 2008, a Comissão Europeia e a *International Telecommunication Union* (ITU) lançaram o projeto *Harmonization of ICT Policies, Legislation and Regulatory. Procedures in the Caribbean* (HIPCAR) com o propósito de fomentar a uniformização da legislação nos países da Comunidade das Caraíbas (CARICOM[102]) em nove áreas[103] relacionadas com tecnologias de informação.

101 Para uma crítica a este dispositivo do anteprojeto, v. Pradillo, 2013: 193-196

102 Da CARICOM fazem parte Antígua e Barbuda, as Bahamas, Barbados, Belize, Domínica, República Dominicana, Grenada, Guiana, Haiti, Jamaica, Monserrate, Santa Lúcia, São Cristóvão e Neces, São Vicente e Grenadinas, Suriname e Trindade e Tobago.

103 A saber, transações eletrónicas, prova digital no comércio eletrónico, privacidade e proteção de dados, interceção de comunicações, cibercrime, acesso a informação pública (liberdade de informação), serviço e acesso universal, interconexão e acesso e, por fim, licenciamento.

O resultado foi possivelmente o mais detalhado modelo legislativo em matéria de cibercrime e prova digital existente, que deverá servir como guião para os diversos Estados que o queiram implementar[104].

Assim, no artigo 27.º do *Cybercrime/e-Crimes Model Policy Guidelines in Legislative Texts*[105], foi criada uma norma que prevê, precisamente, o uso de *malware* em sede de investigação criminal (aí designado *remote forensic software*). Em virtude do carácter altamente intrusivo deste meio, a norma contém certas restrições para a sua aplicação, como sejam, a exigência de que a prova não possa ser obtida de outro modo, a necessidade de precedência de autorização por parte de *juiz ou magistrado*, a exigência de densificação da autorização concedida e a limitação do seu âmbito de aplicação.

À exceção da abertura dada à consagração legal da necessidade de mera precedência de despacho por autoridade judiciária (e não necessariamente judicial) e da ausência de referência expressa à junção aos autos do relatório de

104 Cf. Gercke, 2012: 143.

105 *"Sec. 27 – Forensic Software*
*(1) If a judge is satisfied on the basis of [information on oath/affidavit] that in an investigation concerning an offence listed in paragraph 5 hereinbelow there are reasonable grounds to believe that essential evidence can not be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge/magistrate] [may/shall] on application authorize a police officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:*
*(a) suspect of the offence, if possible with name and address, and*
*(b) description of the targeted computer system, and*
*(c) description of the intended measure, extent and duration of the utilization, and*
*(d) reasons for the necessity of the utilization.*
*(2) Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation it is necessary to log*
*(a) the technical mean used and time and date of the application; and*
*(b) the identification of the computer system and details of the modifications undertaken within the investigation;*
*(c) any information obtained.*
*Information obtained by the use of such software need to be protected against any modification, unauthorized deletion and unauthorized access.*
*(3) The duration of authorization in section 27 (1) is limited to [3 month]. If the conditions of the authorization are no longer met, the action taken is to stop immediately.*
*(4) The authorization to install the software includes remotely accessing the suspects computer system.*
*(5) If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled.*
*(6) If necessary a police officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process.*
*(7) [List of offences]*
*(8) A country may decide not to implement section 27."*

utilização de *malware* (os *logs*), a norma constitui um bom exemplo de técnica legislativa a ser utilizada pelos Estados que pretendam integrar este meio de obtenção de prova no seu catálogo processual.

Por outro lado, e como referimos, também a UE tem – ainda que com pouca ênfase – procurado fomentar a consagração deste meio de obtenção de prova no espaço comunitário.

Desde logo em 2008, por ocasião da adoção da estratégia para reforçar o combate ao cibercrime, o Conselho de Ministros da União Europeia comunicou que a sua estratégia para os cinco anos seguintes incluiria, entre outros, o recurso a ciberpatrulhas para localização, em rede, de criminosos e a pesquisas remotas[106]. Porém, com maior expressividade, fez-se constar no considerando n.º 27 da Diretiva 2011/92/UE do Parlamento Europeu e do Conselho, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, a seguinte previsão: "[o]*s responsáveis pela investigação e pela ação penal relativas aos crimes referidos na presente diretiva deverão dispor de instrumentos de investigação eficazes. Estes instrumentos podem incluir a interceção de comunicações, a vigilância discreta, inclusive por meios eletrónicos, a monitorização de contas bancárias ou outras investigações financeiras, tendo em conta, nomeadamente, o princípio da proporcionalidade e a natureza e gravidade dos crimes investigados*".

Em face da crescente popularidade que este meio de obtenção de prova tem vindo a ganhar, e tendo em conta as suas óbvias vantagens, cremos que a tendência será a de se verificar, nos anos vindouros, um esforço acrescido no sentido da sua consagração pelos diversos Estados-Membros, não só em matéria de combate ao abuso sexual e exploração sexual de crianças e pornografia infantil, mas também quanto a outro tipo de criminalidade grave, como o terrorismo.

## CAPÍTULO III – A UTILIZAÇÃO DE *MALWARE* E A LEI DO CIBERCRIME

### 1. (In)aplicabilidade direta do regime das interceções de comunicações e da pesquisa de dados informáticos

Como ensina Maria de Fátima Mata-Mouros a propósito de alguns novos métodos de investigação criminal nos quais inclui as ditas *buscas online*, "[f]*ruto das incessantes inovações tecnológicas, estes métodos de investigação não cessam de se multiplicar, numa dinâmica que invariavelmente tem como primeiros utilizadores*

106 Disponível em: http://europa.eu/rapid/press-release_IP-08-1827_en.htm?locale=es [consultado em: 10-10-2013].

*os próprios agentes criminosos, para só de seguida motivar agentes policiais e, apenas no fim da cadeia, encontrarem expressão na legislação e no aplicador do direito*"[107].

Assim se explica, cremos, o motivo pelo qual temos assistido recentemente a uma defesa, maioritariamente sustentada por parte de membros de órgãos de polícia criminal – sempre rodeada de secretismo e nunca transposta para o papel –, da admissibilidade, no plano do direito constituído, das ditas *buscas online*, com fundamento, em alguns casos, numa aplicação direta do regime da interceção de comunicações, previsto no artigo 18.º da Lei do Cibercrime, noutros casos, numa aplicação deste regime mesclado com o regime das buscas, assim se *retalhando* por via interpretativa uma base legal apta a legitimar aquele meio de obtenção de prova, e, ainda noutros casos, na aplicação do regime da pesquisa de dados informáticos, previsto no artigo 15.º da Lei do Cibercrime.

Acontece que, como se procurará demonstrar sumariamente, nenhum dos referidos preceitos basta para sustentar a instalação e utilização de *malware* em sistemas informáticos utilizados por suspeitos da prática de ilícitos criminais.

Desde logo, no que respeita à interceção de comunicações, compulsado o artigo 18.º da Lei do Cibercrime e, bem assim, o regime das escutas telefónicas para o qual remete o seu n.º 4, não logramos encontrar qualquer base legal que permita sustentar a instalação remota de *malware* com vista à obtenção de dados informáticos. Pelo contrário, qualquer dos normativos em causa permite que se *intercetem* comunicações, isto é, que se captem as comunicações visadas entre o momento do seu envio pelo remetente e o momento da sua chegada ao destinatário; nunca a monitorização de dados diretamente no aparelho utilizado para as enviar, onde, em rigor, como se verá *infra*, não estamos (ou não estamos somente) perante *comunicações*[108]. Argumentar-se-ia, porém, que, nos termos do artigo 189.º do CPP se encontram previstas as escutas ambientais, as quais pressupõem, à semelhança do uso de *malware*, a instalação em espaços físicos de meios técnicos, de modo secreto, com vista à captação de conversações

107 Mata-Mouros, 2011: 433.

108 Neste sentido, referiu o Tribunal Constitucional alemão, no citado acórdão de 27 de fevereiro de 2008, que "[s]*e um sistema informático complexo for tecnicamente infiltrado de modo a realizar-se vigilância de telecomunicações ("source telecommunication surveillance"), a infiltração ultrapassa o obstáculo crítico à espionagem do sistema como um todo. O perigo assim trazido excede em muito o que é provocado pela mera vigilância de telecomunicações em curso. Em particular, os dados armazenados em computadores privados que não se relacionem com o uso do sistema para telecomunicação também podem ser obtidos. Por exemplo, o ato de utilizar o computador pessoal para fins pessoais, a frequência de acesso a certos serviços, em particular, também os conteúdos ou ficheiros criados ou – na medida em que o sistema informático infiltrado também controle aparelhos elétricos em casas – a conduta na habitação pessoal pode ser descoberta*".

diretamente na sua origem. Todavia, e sem prejuízo de mais argumentos de índole substantiva existirem quanto a esta matéria, dir-se-á tão-somente que a remissão feita pelo legislador no n.º 4 do artigo 18.º da Lei do Cibercrime para o regime das escutas se restringe – como aí se diz – ao "*regime de interceção e gravação de conversações ou comunicações* ***telefónicas*** *constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal*", e não ao regime de extensão previsto no artigo 189.º do CPP, o qual foi excluído pelo legislador.

Com efeito, tendo em conta que a recolha de prova por esta via é feita em dois momentos – o da instalação do *malware* e o da sua utilização –, não só não pode ignorar-se o método altamente invasivo utilizado para obter a informação visada diretamente na sua fonte, como não pode ignorar-se que, contrariamente à interceção de comunicações – limitada no tipo de dados a intercetar –, dificilmente se poderá defender que o uso de *malware* apenas permite (ou pretende) captar um conjunto específico de dados. Pelo contrário, permite monitorizar toda a atividade, lícita e ilícita, empreendida no computador do visado ou em torno do mesmo (pense-se na ativação da *webcam* ou do microfone), subsumível, ou não, ao conceito de comunicação. Mais, perguntar-se-á, onde se pode encontrar nos citados normativos legais alegadamente aplicáveis, a base legal para a instalação de *keyloggers* que visem captar as credenciais de acesso a documentos cifrados no computador do visado?

Com efeito, o uso de *malware* não visa verdadeiramente intercetar comunicações. Pelo contrário, para a interceção de comunicações existe, precisamente, o regime do artigo 18.º da Lei do Cibercrime. Assim, como refere Costa Andrade a propósito daquilo que qualifica de *busca online*, "[s]*endo ela própria um ato de telecomunicação e suposto que o computador-alvo esteja ligado à* internet[109], *ela não incide nem recai sobre um ato de telecomunicação. É, em síntese, uma ação de telecomunicação cujo objeto não é telecomunicação. Uma agressão através da telecomunicação não é necessariamente uma agressão à liberdade de telecomunicação*"[110]. Assim, "*a busca* online, *porque não configura uma invasão ou devassa de um ato de telecomunicação, não está abrangida nem legitimada pelas normas da lei processual relativas às intromissões nas telecomunicações*"[111].

109 Não subscrevemos inteiramente este primeiro segmento, uma vez que, como se viu, é concebível a infeção de um sistema informático desconectado da Internet.

110 Andrade, 2009a: 168.

111 Andrade, 2009a: 160.

Destarte, uma vez que não existe supedâneo legal que legitime o meio de obtenção de prova em apreço, não é lícito ao intérprete criar uma nova norma na qual possa *encaixar* um meio de obtenção de prova atípico – especialmente um meio de obtenção de prova oculto –, ignorando os limites legais e constitucionais à sua utilização. Até porque, como ensina Paulo de Sousa Mendes, "*o catálogo dos meios de prova típicos inclui os respetivos regimes e não permite que sejam desrespeitadas as suas regras, a fim de serem criados meios de prova aparentados mas atípicos.* […] *Portanto, a única liberdade que existe relativamente à escolha dos meios de prova consiste na possibilidade de selecionar do catálogo dos meios de prova típicos aqueles que forem considerados como adequados ao processo em curso*"[112].

Por outro lado, como se referiu, alguma doutrina vem sustentando nesta matéria que, com a consagração do artigo 15.º da Lei do Cibercrime, o legislador pretendeu introduzir no ordenamento jurídico português as chamadas *buscas online*.

Neste sentido, sustenta Paulo Pinto de Albuquerque que "[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' por despacho da autoridade judiciária ou mesmo decisão do órgão de polícia criminal. A lei não coloca quaisquer restrições relativamente aos conteúdos dos dados que podem ser pesquisados, ao invés do que sucede na apreensão de dados informáticos. A lei nova também não exige que a pesquisa informática ordenada pelo MP ou pelo OPC seja validada pelo juiz. Esta intrusão na privacidade da pessoa visada é 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 atos instrutórios que representem uma intrusão na privacidade*[113].

Não obstante seja inevitável a conclusão pela inconstitucionalidade a que chega o Autor em face dos pressupostos que apresenta, não podemos deixar de assinalar que, segundo cremos, esses pressupostos não se verificam, pelo que e, como tal, não existe necessidade de formular semelhante juízo sobre a norma do art. 15.º.

Em primeiro lugar, porque o n.º 1 do artigo 15.º da Lei do Cibercrime se refere à obtenção "*de dados informáticos específicos e determinados, armazenados num determinado sistema informático*", o que exclui, desde logo, a obtenção genérica de dados em tempo real. Em segundo lugar, porque mesmo a admissibilidade da extensão da pesquisa informática a sistemas acessíveis através de

112 Mendes, 2013: 174 e, em sentido semelhante, Neves, 2011: 98-99.

113 Neste sentido, cf. Albuquerque, 2011: 502.

outro sistema que seja inicialmente objeto da pesquisa, nos termos do n.º 5 do artigo 15.º da Lei do Cibercrime, não permite extrair esta conclusão, uma vez que o que esta extensão implica é que o acesso ao segundo sistema informático tem de ser feito através do primeiro sistema pesquisado, e não a partir de um qualquer outro sistema utilizado pelo investigador criminal. Por fim, não só o artigo 15.º é totalmente omisso quanto à instalação por via remota de qualquer *software* no computador do visado, como o próprio facto de o artigo se referir à realização da pesquisa "*nesse sistema*" e de remeter para as regras de execução das buscas previstas no CPP (em particular para o n.º 1 do artigo 176.º deste diploma), indica claramente que a pesquisa é sempre efetuada fisicamente no próprio sistema, salvo no caso previsto no n.º 5 do artigo 15.º da Lei do Cibercrime, em que a pesquisa é feita por via remota a outro sistema informático mas tendencialmente a partir do sistema inicialmente objeto da pesquisa.

Assim sendo, será de concluir pela inaplicabilidade de qualquer uma das referidas normas para sustentar a utilização de *malware* no contexto de investigações criminais em ambiente digital.

## 2. A utilização de *malware* no contexto de ações encobertas em ambiente digital

Problema diverso, como tivemos ocasião de referir brevemente, é o da utilização de *malware* no contexto de ações encobertas em ambiente digital.

Com efeito, numa medida que entendemos de louvar quanto às suas originalidade e utilidade[114], e de censurar, por um lado, quanto à sua consagração por mera remissão para o regime da Lei n.º 101/2001, de 25 de agosto, e, por outro, quanto ao seu excessivamente alargado âmbito objetivo de aplicação, o legislador veio introduzir, no artigo 19.º, n.º 1, da Lei do Cibercrime, a figura do agente encoberto em ambiente digital.

No número 2 do referido preceito, o legislador introduziu uma norma que reza o seguinte: "[s]*endo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações*". Trata-se de uma disposição formulada em termos muitíssimo vagos, introduzida como última norma do regime processual penal em matéria de prova digital e sistematicamente inserida num artigo relativo a uma figura jurídica (o agente encoberto) utilizada em casos excecionais. Estas circunstâncias

114 Fê-lo, sublinha-se, sem que tal constasse da Convenção sobre o Cibercrime ou da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação.

justificam, segundo cremos, que a norma não tenha recebido particular atenção por parte da doutrina, sendo comummente desconsiderada ou encarada como uma norma que visa tão-somente facultar aos órgãos de polícia criminal meios técnicos indefinidos, em certa medida análogos à interceção de comunicações, a utilizar no contexto das ações encobertas em ambiente digital.

Contudo, se no plano formal esta formulação pode aparentar ser satisfatória e inócua, a verdade é que uma análise mais profunda, focada na concretização, no plano operacional, destes "*meios e dispositivos informáticos*" leva-nos a concluir que estamos perante (i) um novo meio (oculto) de obtenção de prova e (ii) um meio particularmente gravoso de investigação.

Ora, a novidade deste meio decorre, desde logo, do facto de os "*meios e dispositivos informáticos*" aqui referidos não se subsumirem a qualquer um dos meios de obtenção de prova previstos na legislação processual penal portuguesa. Esta conclusão impõe-se pelo mero facto de o legislador ter sentido necessidade de introduzir uma norma nova para legitimar o recurso a estes meios e dispositivos informáticos. Uma norma que terá surgido em face da insuficiência dos demais meios processuais existentes para a utilização destes "*meios e dispositivos informáticos*"[115].

Entendimento diverso implicaria que o legislador tivesse introduzido neste dispositivo uma norma redundante e supérflua que visasse tão-somente ao agente encoberto recorrer a quaisquer outros "*meios e dispositivos informáticos*" existentes – o que é afastado pela própria letra da norma que remete o intérprete, "*naquilo que for aplicável*", para o regime da interceção de comunicações.

Quanto ao caráter particularmente gravoso da utilização destes "*meios e dispositivos informáticos*" bastará referir que, por força da sua inserção sistemática, o recurso aos mesmos encontra-se limitado ao contexto excecional das ações encobertas, sendo que, mesmo nesse âmbito, apenas podem ser aplicados "*se necessário*" (artigo 19.º, n.º 2, da Lei do Cibercrime), bem como "*se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter*", devendo ser precedidos de despacho fundamentado do juiz de instrução a proferir mediante requerimento do Ministério Público (artigo n.º 18.º, n.º 2, aplicável *ex vi* artigo 19.º, n.º 2, da Lei do Cibercrime).

115 Não se trata, por isso, dos *"dispositivos electromagnéticos, acústicos, mecânicos ou outros"* utilizados para preenchimento do conceito de interceção, nos termos do artigo 2.º, alínea *e)* da Lei do Cibercrime.

Com efeito, tendo em conta que (i) o agente encoberto será um dos métodos ocultos de investigação com maior grau de lesividade e de devassa, e que (ii) a utilização de quaisquer métodos ocultos obedece a uma lógica de subsidiariedade (i.e., só se recorre ao meio mais gravoso, se não for possível o recurso a meios menos gravoso)[116], a própria existência de uma previsão autorizando a utilização, sujeita a critérios de necessidade e subsidiariedade, de um determinado método de investigação no contexto das acções encobertas, indica que se tratará de um meio com um grau de lesividade e devassa superior às próprias ações encobertas.

Perguntar-se-á, então, novamente, que "*meios e dispositivos informáticos*" serão estes? A resposta, como se viu, implica que tenhamos em consideração que se trata de meios e dispositivos que não encontram previsão expressa na lei processual penal portuguesa por cujo carácter excecional, invasivo e insidioso possa ser comparado e condicionado ao recurso ao agente encoberto e cujo funcionamento possa ser regulado e limitado pelo regime da interceção de comunicações. Trata-se, a nosso ver, da consagração da utilização (que incluirá, naturalmente, a instalação) de *malware* como método oculto de investigação criminal em ambiente digital.

Veja-se, aliás, a título meramente ilustrativo, que a terminologia adotada pelo legislador português, não só permite englobar o *malware*, como é em muito semelhante à utilizada em diplomas de outros ordenamentos jurídicos para consagrar este mesmo método. Não só é o caso dos "*meios técnicos*" incluídos no citado artigo 5.2 (11) da Lei de Proteção da Constituição da Renânia do Norte-Vestefália, como dos "*dispositivos técnicos*" do artigo 706-101-1 do Código de Processo Penal francês, ou dos "*dispositivos de vigilância de dados*" (*data surveillance device*) previstos no artigo 6.º do *Surveillance Devices Act* australiano, como ainda dos "*meios eletrónicos*" para vigilância discreta previstos no citado Considerando n.º 27 da Diretiva 2011/92/UE do Parlamento Europeu e do Conselho, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, a seguinte previsão.

Assim, se concluirmos que o conceito de "*utilização*" de meios e dispositivos previsto no artigo 19.º, n.º 2, inclui o conceito de *instalação* – o que, admitindo que estes meios e dispositivos são, na verdade, *malware*, não suscitará dúvidas –,

116 Cf. Andrade, 2009a: 115, 2009b: 542-546, e, Mata-Mouros, 2011: 224-229.

restar-nos-á concluir que o artigo 19.º, n.º 2 prevê o uso, no contexto de ações encobertas, desta nova "*intervenção encoberta em sistemas informáticos*"[117].

De uma leitura conjugada do regime do agente encoberto e do regime da interceção de comunicações, decorrem, pelo menos, os seguintes requisitos para a utilização de *malware*:

a) Adequação aos fins de prevenção[118] e repressão criminais identificados em concreto e proporcionais, quer a essas finalidades, quer à gravidade do crime sob investigação (artigo 3.º, n.º 1, da Lei n.º 101/2001, de 25 de agosto);
b) Fundadas suspeitas da prática de um dos crimes previstos na Lei do Cibercrime ou de crimes cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos (artigo 19.º, n.º 1, da Lei do Cibercrime);
c) A sua utilização apenas pode ocorrer quando houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter (artigo 18.º, n.º 2, da Lei do Cibercrime);
d) A precedência de despacho fundamentado do juiz de instrução, mediante requerimento do Ministério Público (artigo 18.º, n.º 2 da Lei do Cibercrime). Não admitimos, portanto, nesta matéria, uma *reserva* de juiz como a que existe no contexto das ações encobertas de repressão (traduzida numa espécie de *deferimento tácito judicial* decorridas que sejam 72 horas desde a comunicação da sua realização ao juiz de instrução), embora a inserção sistemática da norma e a sua redação com uma mera remissão

117 Rogall, 2010: 120.

118 Cumpre alertar para o facto de que a adequação aos fins de prevenção não legitima, no plano do direito constituído, o uso de *malware* em ações encobertas de natureza preventiva, desde logo porque se, por um lado, estas ações poderiam aparentar ser admissíveis ao abrigo do disposto no artigo 3.º, n.º 4, da Lei n.º 101/2001, de 25 de agosto, por outro lado, o artigo 18.º, n.º 2, da Lei do Cibercrime refere expressamente que "[a] *interceção e o registo de transmissões de dados informáticos só podem ser autorizados* ***durante o inquérito***".

"*naquilo que for aplicável*" para o regime das interceções, abra uma *janela* perigosa[119].

e) A delimitação dos dados que se visa obter, de acordo com as necessidades concretas da investigação (artigo 18.º, n.º 3 da Lei do Cibercrime).

Respeitados os requisitos *supra* elencados, nada pareceria obstar, no plano do direito constituído, à utilização de *malware* como meio de obtenção de prova em ambiente digital.

Veremos, porém, se assim sucede.

### 3. A utilização de *malware* como medida restritiva de direitos fundamentais e consequente necessidade de densificação normativa

Não obstante defendamos a necessidade do recurso a *malware* como meio de obtenção de prova em processo penal, a verdade é que, como procuraremos demonstrar, ainda que muito sinteticamente e a título introdutório, não podemos concordar com os moldes em que o mesmo foi consagrado na legislação portuguesa.

Com efeito, a instalação de *malware* será, possivelmente, a par do recurso ao agente encoberto, o meio mais gravoso de obtenção de prova suscetível de merecer consagração legal num Estado de direito democrático. O elevado nível de danosidade social que a monitorização remota da conduta privada de um indivíduo no seu computador representa – talvez até acompanhada da captação de imagens e som do visado com recurso a esse mesmo sistema informático, numa intromissão potencialmente inadmissível no núcleo intangível da intimidade pessoal –, aliado à gravíssima ofensa dos seus direitos fundamentais à reserva da intimidade da vida privada, à inviolabilidade do domicílio, à confidencialidade, à imagem, à palavra e ainda, como acima se viu, à confidencialidade e integridade dos sistemas de informação, justifica que a consagração legal desta norma revista especial densidade, bem como que as funcionalidades do meio técnico a usar obedeçam a limites claros e específicos, em obediência ao princípio da proporcionalidade[120].

Assim, não basta que exista uma norma que, de forma genérica – e ainda que por remissão para outro regime –, confira supedâneo legal à utilização de

119 A propósito da necessária reserva de juiz dos métodos ocultos de investigação criminal, cf. Andrade, 2009b: 546-551.

120 Rodrigues, 2010: 474-475.

*malware*, porquanto, em medidas desta natureza, quase tão importante quanto a reserva de lei é a reserva de precisão legal[121]. E este dever de precisão legal não é compatível com a mera criação de um meio de investigação cujos funcionamento e finalidade não sejam sequer referidos – quanto mais limitados – na própria norma que os prevê.

A *ultima ratio*, mesmo dentro dos meios ocultos de investigação criminal, que está subjacente à utilização de *malware* não se compadece com uma mera referência à sua necessidade, seguida de uma remissão genérica "*naquilo que for aplicável*" para um regime legal que, por sua vez, remete "[e]*m tudo o que não for contrariado*" para outro regime.

Aliás, como vem recorrentemente afirmando o TEDH nesta matéria, para cumprimento dos requisitos impostos pelo artigo 8.º da CEDH, não basta a existência de previsão legal, é necessária a imposição de "*qualidade da lei*" que torne as medidas processuais acessíveis e previsíveis, de modo a que o cidadão possa conhecer as condições, limites e circunstâncias em que as mesmas podem ser aplicadas. Adicionalmente, deverá a norma ser clara e precisa, permitindo o conhecimento da finalidade que prossegue e das modalidades que admite, o que servirá, acima de tudo, para conceder meios de tutela contra a sua utilização arbitrária[122].

Do mesmo modo, para cabal cumprimento do disposto no artigo 18.º n.º 2, da CRP, cabe ao legislador impor uma especial densidade aos pressupostos legais deste método oculto de investigação, dotando a norma em apreço de especial clareza, precisão e previsibilidade. Não o fazendo, e sem prejuízo de outros vícios que uma análise mais aprofundada possa revelar, a norma afigura-se inconstitucional, por violação do disposto nas disposições conjugadas dos artigos 18.º, n.º 2, 26.º, n.º 2, e 1.º da CRP.

## 4. Sindicância da prova obtida através do uso de *malware*

Entre várias perplexidades, a análise do disposto no artigo 19.º, n.º 2, da Lei do Cibercrime suscita uma de particular gravidade, porquanto intrinsecamente ligada à salvaguarda das garantias do arguido: a da publicidade do meio de obtenção de prova utilizado.

121 Cf. Mata-Mouros, 2011: 38, 123-126, 242-252.

122 Nesta matéria v. caso Malone v. Reino Unido (pedido n.º 8691/79) e caso Vetter c. France (Pedido n.º 59842/00).

Com efeito, por um lado, o recurso a "*meios e dispositivos informáticos*" encontra-se, por força da sua inserção sistemática, condicionado ao recurso prévio ao agente encoberto. Por outro lado, ao recurso a "*meios e dispositivos informáticos*" é aplicável o regime da interceção de comunicações e, por remissão deste, o das escutas telefónicas. Acontece que o regime legal em vigor não garante ao arguido o conhecimento da existência de uma ação encoberta.

Porém, o regime das escutas telefónicas, no seu artigo 188.º, n.º 8, aplicável *ex vi* artigo 18.º, n.º 4, da Lei do Cibercrime, prevê que "[a] *partir do encerramento do inquérito, o assistente e o arguido podem examinar os suportes técnicos das conversações ou comunicações e obter, à sua custa, cópia das partes que pretendam transcrever para juntar ao processo, bem como dos relatórios previstos no n.º 1, até ao termo dos prazos previstos para requerer a abertura da instrução ou apresentar a contestação, respetivamente*".

Assim, se entendermos a remissão do artigo 19.º, n.º 2, para o artigo 18.º, ambos da Lei do Cibercrime, como incluindo a remissão para o regime das escutas telefónicas do artigo 188.º do CPP, poderemos cair no absurdo de não ser divulgada ao arguido a existência de uma ação encoberta, mas, simultaneamente, de terem de lhe ser facultados os suportes técnicos nos quais se encontra armazenada a prova recolhida com recurso a *malware*, quando o uso de *malware* apenas seria permitido no contexto de ações encobertas que, por sua vez, podem não ser reveladas.

Tal perplexidade, porém, não poderá fundamentar a prevalência da regra aplicável às ações encobertas e a consequente não divulgação da utilização de *malware* como meio de obtenção de prova num determinado procedimento criminal. E não poderá desde logo porque – a menos que outro interesse de superior relevo a tal impeça (como, no caso do agente encoberto, a segurança do próprio agente) – quaisquer diligências que constituam uma atividade instrutória intrusiva têm obrigatoriamente de constar dos autos sob pena de violação intolerável das garantias de defesa do arguido. Ademais, tratando-se de prova digital, a sua volatilidade e fragilidade impõem requisitos de verificação de fidedignidade e de garantia da cadeia de custódia que podem não existir com a prova comummente recolhida por agentes encobertos.

Aliás, como se viu, poderemos estar perante prova contaminada pelos *supra* referidos ataques contra perícias forenses[123], perante *malware* corrompido ou

123 Os quais, segundo van Buskirk e Liu têm uma presunção de fidedignidade imerecida, *apud* Kessler, 2007.

com deficiências técnicas aptas a retirar fiabilidade à prova, ou mesmo porque o próprio sistema informático no qual o órgão de polícia criminal instala *malware* pode estar já infetado com outro tipo de *malware* que permite a um terceiro controlar aquele sistema informático, assim incriminando o visado pela investigação – a chamada *Trojan horse defence*[124].

Por outro lado, o fundamento para a proteção do agente encoberto, subjacente à não revelação da mera existência destas acções, não se verifica com a mesma intensidade no caso de agentes encobertos em ambiente digital, uma vez que os mesmos, se omitirem a sua identidade durante o decurso da investigação, muito dificilmente poderão ser identificados por aqueles que forem incriminados por a prova assim recolhida.

Dado que o acesso à informação mediante a qual foi recolhida a prova digital é essencial para a sua sindicância e consequente verificação da sua fidedignidade, resta concluir que a eventual ocultação do recurso a *malware*, bem como a omissão de referência no processo ao tipo de *malware* concretamente utilizado e ainda a eventual vedação ao arguido de exame da prova assim recolhida, violam de forma intolerável as suas garantias de defesa e o seu direito ao contraditório, previstos no artigo 32.º, n.os 1 e 5, da CRP.

## CONCLUSÕES

O recurso a *malware* como meio de obtenção de prova penal reveste uma utilidade e eficácia sem paralelo no contexto de investigações criminais em ambiente digital. Com efeito, o advento das técnicas antiforenses, aliado à sua democratização e facilidade de utilização, têm vindo a dificultar seriamente o combate ao cibercrime, pelo que, nos casos da criminalidade mais grave, se torna urgente a imposição de medidas de carácter mais gravoso para a sua prossecução.

Evidência da utilidade deste meio de obtenção de prova é, não só a sua utilização por vários Estados a nível mundial, mas também a crescente tendência para a sua consagração num espectro cada vez mais alargado de Estados, por vezes com base em iniciativas de cariz *supra* nacional que visam uniformizar os seus requisitos.

Foi, ao que nos parece, com o intuito de consagrar o recurso ao *malware* que o legislador consagrou o recurso a "*meios e dispositivos informáticos*" no

124 Cf. Brenner, Carrier & Henninger,2004: 1-53 e Clough, 2010: 34.

contexto de ações encobertas em ambiente digital, no artigo 19.º, n.º 2, da Lei do Cibercrime.

Fê-lo, porém, de modo dúbio, excessivamente vago e com um elevado défice de clareza, previsibilidade e precisão legal, em violação do disposto nos artigos 18.º, n.º 2, 26.º, n.º 2, e 1.º da CRP, assim permitindo interpretações díspares quanto aos seus pressupostos e requisitos e proporcionando as circunstâncias adequadas a que a sua utilização seja omitida nos autos ou mesmo, em geral, do conhecimento público. Fê-lo em prejuízo das garantias de defesa e do direito ao contraditório do arguido, numa área onde a prova reveste particular fragilidade. Destarte, também aqui a referida norma poderá enfermar do vício de inconstitucionalidade, por violação do disposto no artigo 32.º, n.os 1 e 5, da CRP.

Com efeito, para uma consagração leal de um meio de prova tão insidioso e gravemente restritivo de direitos fundamentais do visado, deverá o legislador prever, de forma lisa, transparente e suficientemente densificada, os pressupostos, requisitos e finalidades da instalação e utilização de *malware* como meio de obtenção de prova em processo penal.

**BIBLIOGRAFIA**

Abel, Wiebke & Schafer, Burkhard

2009 "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822" *SCRIPTed – A Journal of Law, Technology & Society*, Vol. 6, n.º 1, pp. 106-123.

Adleman, Leonard M.

1988 "An Abstract Theory of Computer Viruses", *Advances in Cryptology – CRYPTO 88*, Vol. 403, pp. 354-374.

Albuquerque, Paulo Pinto de

2011 *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4.ª ed., Lisboa: Universidade Católica Editora.

Andrade, Manuel da Costa

2009a *"Bruscamente no Verão passado" a Reforma do Código de Processo Penal – Observações Críticas sobre uma Lei que Podia e Devia ter sido Diferente*, Coimbra: Coimbra Editora.

2009b "Métodos ocultos de investigação (Plädoyer para uma teoria geral), *Que futuro para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*", Coimbra: Coimbra Editora, pp. 525-551.

Aquilina, James M., Casey, Eoghan & Malin, Cameron H.

2008 *Malware Forensics: Investigating and Analyzing Malicious Code*, EUA: Elsevier.

Aycock, John

2006 *Computer Viruses and Malware*, EUA: Springer.

Berinato, Scott

2007 "The Rise of Anti-Forensics", *CSOOnline*, disponível em: http://www.csoonline.com/article/221208/the-rise-of-anti-forensics [consultado em: 05.10.2013].

Bettini, Claudio*, et al.*

2009 *Privacy in Location-Based Applications: Research Issues and Emerging Trends*, Heidelberg: Springer-Verlag Berlin.

Bickford, Jeffrey, *et al*.

2010 "Rootkits on Smart Phones: Attacks, Implications and Opportunities", *Proceedings of the 11th International Workshop on Mobile Computing Systems and Applications*, Annapolis, Maryland, pp. 49-54.

Boldt, Martin

2010 *Privacy-Invasive Software*, Karlskrona: Blekinge Institute of Technology.

Brenner, Susan W.
2012 "Law, Dissonance and Remote Computer Searches", *North Carolina Journal of Law and Technology*, Vol. 14, n.º 1, pp. 43-92.
Brenner, Susan W., Carrier, Brian & Henninger, Jef
2004 "The Trojan horse defense in cybercrime cases", *Santa Clara Computer and High Technology Journal*, Vol. 24, pp. 1-53.
Casey, Eoghan
2011 *Digital Evidence and Computer Crime, Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet*, 3.ª ed., Califórnia: Elsevier.
Clough, Jonathan
2010 *Principles of Cybercrime*, Cambridge: Cambridge University Press.
Correia, Miguel Pupo & Sousa, Paulo Jorge
2010 *Segurança no Software*, Lisboa: FCA – Editora de Informática.
Curran, Kevin, *et al.*
2008 "Hacking and Eavesdropping", *Cyber Warfare and Cyber Terrorism* (org. Lech J. Janczewski e Andrew M. Colarik), Nova Iorque: Information Science Reference.
Davis, Michael, Bodmer, Sean & Lemasters, Aaron
2010 *Hacking Exposed – Malware & Rootkits: Malware & Rootkits Security & Secret Solutions*, EUA: McGraw-Hill.
Dingledine, Roger, Mathewson, Nick & Syverson, Paul
2004 "Tor: The Second-Generation Onion Router", *Proceedings of the 13th USENIX Security Symposium – August 9-13, 2004, The USENIX Association*, disponível em: http://static.usenix.org/event/sec04/tech/full_papers/dingledine/dingledine.pdf [consultado em: 09.06.2012].
Erbschloe, Michael
2005 *Trojans, Worms and Spyware – A Computer Security Professional's Guide to Malicious Code*, EUA: Elsevier.
Filiol, Eric
2005 *Computer viruses: from theory to applications*, França: Springer.
Garitaonandia, Iñaki Esparza Leibar y Alberto Saiz
2010 "La intervención de las comunicaciones en el derecho comparado: los casos de Francia e los Estados Unidos de America", in AA.VV. *Derecho Penal Informático* (Dir. José Cuesta Arzamendi), Pamplona: Thomson Reuters, pp. 321-345.
Gercke, Marco
2012 *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, Telecommunication Development Sector.

Gradigo, Will, *et al.*
2013 *Blackhatonomics – Na Inside Look at the Economics of Cybercrime*, EUA: Elsevier.
Graham, James, Howard, Richard & Olson, Ryan
2011 *Cyber Security Essentials*, Boca Raton: Taylor and Francis.
Grinberg, Reuben
2011 "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science and Technology Law Journal*, Vol. 4, n.º 1, pp. 159-208.
Harris, Ryan
2006 "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", *Digital Investigation – The International Journal of Digital Forensics & Incident Response*, Vol. 3 – Suplemento, pp. 44-49.
Kessler, Gary C.
2007 "Anti-Forensics and the Digital Investigator", Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia.
Landau, Susan
2010 *Surveillance or Security – The risks Posed by new Wiretapping Technologies*, EUA: MIT Press.
López, Mercedes Fernández
2011 "Algunas propuestas para regular la investigación del Cibercrimen", in AA.VV. *La Reforma del Proceso Penal*, Madrid: La Ley, pp. 269-292.
Mata-Mouros, Maria de Fátima
2011 *Juiz das Liberdades – Desconstrução de um Mito do Processo Penal*, Coimbra: Almedina.
Mcafee
2006 Rootkits, *Part 1 of 3: The Growing Threat*, White Paper.
Mendes, Paulo de Sousa
2013 *Lições de Direito Processual Penal*, Coimbra: Almedina.
Mesquita, Paulo Dá
2010 *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Wolters Kluwer.
Mohay, George, *et al.*
2003 *Computer and Intrusion Forensics*, Massachusetts: Artech House, Inc.
Morton, K. F. & Grace, David
2012 "A Case Study on Stuxnet and Flame Malware", disponível em: http://vixra.org/pdf/1209.0040v1.pdf [consultado em: 03-10-2013].

Murphy, Angela
2002 "Cracking the Code to Privacy: How Far Can the FBI Go?", *Duke Law & Technology Review*, n.º 1, disponível em: http://scholarship.law.duke.edu/cgi/viewcontent.cgi? article=1043&context=dltr [consultado em: 08.10.2013].
Neves, Rita Castanheira
2011 *As ingerências nas comunicações electrónicas em processo penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra: Coimbra Editora.
Nuñez, Eloy Velasco
2010 *Delitos cometidos a través de Internet. Cuestiones procesales*, Madrid: La Ley.
2011 «ADSL y Troyanos: Intervención de sus datos y telecomunicaciones en la investigación penal», *La Ley Penal*, n.º 82, pp.18-25.
Patil, Nilesh & Lingam, Chelpa
2012 "Anonymous Connections and Onion Routing", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. II, n.º 2.
Pradillo, Juan Carlos Ortiz
2009 "Remote Forensic Software as a Tool for Investigating Cases of Terrorism", *ENAC – E-newsletter on the fight against cybercrime*, n.º 4, pp. 1-8.
2012 "'Hacking' legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delinquencia informática", *Delincuencia Informática. Tiempos de Cautela y Amparo*, Navarra: Thomson Reuters Aranzadi, pp. 177-220.
2013 *Problemas Procesales de la Ciberdelincuencia,* Madrid: Editorial Colex
Poulsen, Kevin
2013 "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack", Wired, disponível em: http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/[consultado em 05.10.2013].
Ramalho, David Silva
2014 "A investigação criminal na *Dark Web*", *Revista de Concorrência & Regulação,* Ano IV, n.º s 14/15, pp. 383-429.
Rodrigues, Benjamim Silva
2010 *Da Prova Penal – Tomo II – Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, Lisboa: Rei dos Livros.
Rogall, Klaus,
2009 "A nova regulamentação da vigilância das telecomunicações na Alemanha", in AA.VV., *2.º Congresso de Investigação Criminal* (Coordenação Científica: Maria Fernanda Palma *et al*), Coimbra: Almedina, pp. 177-220.

Rosenbach, Marcel
2011 "The shady past of Germany's Spyware", Spiegel Online International, acedido e consultado em 28-08-2012, em http://www.spiegel.de/international/germany/trojan-trouble-the-shady-past-of-germany-s-spyware-a-792276.html.
Santos, Paulo, *et al.*
2008 *Cyberwar – O Fenómeno, as tecnologias e os actores*, Lisboa: FCA – Editora de Informática.
Santos, Osvaldo
2011 *Firewalls – Soluções Práticas*, Lisboa: FCA – Editora de Informática.
Serrano, Nicolas González-Cuellar
2006 "Garantías constitucionales de la persecución penal en el entorno digital", in AA.VV. *Derecho Y Justicia Penal en el Siglo XXI – Liber Amicorum en Homenaje al Profesor Antonio González-Cuellar Garcia*, Madrid: Editorial Colex, pp. 887-916.
Sheetz, Michael
2007 *Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers*, John Wiley & Sons.
Sikorski, Michael & Honig, Andrew
2012 *Practical Malware Analysis – The Hands-on Guide to Dissecting Malicious Software*, San Francisco: No Starch Press.
Sinrod, Eric J. & Reilly, William P.
2000 "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws", *Santa Clara Computer and High Technology Law Journal*, Vol. 16, n.º 2, pp.177-232.
Soghoian, Christopher
2009 "Caught In The Cloud: Privacy, Encryption, And Government Back Doors In The Web 2.0 Era", *J. ON TELECOMM. & HIGH TECH. L.*, Vol. 8, Berkman Center Research Publication, pp. 359-424.
Urbas, Gregor & CHOO, Kim-Kwang
2008 "Resource Materials on Technology-Enabled Crime", *Technical and Background paper*, n.º 28, Canberra: Australian Institute of Criminology, pp. 1-88.
Vaciago, Giuseppe
2012 *Digital Forensics, Italian Criminal Procedure and Due Process Rights in the Cyber Age*, Torino: G. Giappichelli Editore.
Vieira, José Alberto
2009 "Download de obra protegida pelo Direito de Autor e uso privado", *Direito da Sociedade da Informação – Vol. VIII*, Coimbra: Coimbra Editora, pp. 421-467.

Wallace, Benjamin
2011 "The Rise and Fall of Bitcoin", Wired Magazine, disponível em: http://www.wired.com/magazine/2011/11/mf_bitcoin/2/[consultado em: 04-10-2013].
Weber, Rolph H. & Heinrich, Ulrike I.
2012 *Anonymization*, Londres: Springer.
Woo, Cristopher & Miranda, SO
2002 "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance", *Harvard Journal of Law & Technology*, Vol. 15, n.º 2, pp. 521-538.
Zúquete, André
2013 *Segurança em redes informáticas*, 4.ª ed., Lisboa: FCA – Editora de Informática.