Universidade Católica Portuguesa
Faculdade de Direito - Escola de Lisboa
Mestrado Forense

DA PROBLEMÁTICA DA INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL - EM ESPECIAL, SOBRE A POSSIBILIDADE DE UTILIZAÇÃO DE *MALWARE* COMO MEIO OCULTO DE OBTENÇÃO DE PROVA

Dissertação de Mestrado orientada pelo Senhor Professor Doutor Germano Marques da Silva

Maria Ana Barroso de Moura da Silveira
28 de Março de 2016

INDÍCE

ABREVIATURAS

ASFICPJ - Associação Sindical dos Funcionários de Investigação Criminal da Polícia Judiciária

CIJC – Centro de Investigação Jurídica do Ciberespaço

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

FBI – Federal Bureau of Investigation (Agência Federal de Investigação)

INE – Instituto Nacional de Estatística

ISEM – Instituto de Estudos Superiores Militares

LC – Lei do Cibercrime

MP – Ministério Público

ONG – Organização Não Governamental

OPC – Órgão de Polícia Criminal

Proc. – Processo

TC – Tribunal Constitucional

1. Introdução

O rápido e constante progresso e desenvolvimento tecnológico que se tem verificado nas últimas décadas coloca, cada vez mais, problemas práticos ao nível da investigação criminal, tornando mais complexa a recolha e a valoração dos meios de prova, nomeadamente no que diz respeito às actividades criminais que se têm vindo a desenvolver no espaço digital. As especificidades do meio digital implicam necessariamente a previsão de dispositivos processuais específicos para o combate à criminalidade informática. Nesta matéria, os tradicionais meios de obtenção de prova têm-se revelados insuficientes para fazer face aos desafios que a revolução tecnológica coloca ao investigador criminal. O Estado Português procurou dar resposta a este problema com a aprovação da Lei do Cibercrime, prevendo esta lei um conjunto de disposições processuais de obtenção de prova específicas para o ambiente digital. Ainda assim, julgamos, que ainda há um longo percurso legislativo a percorrer, que permita não só harmonizar a legislação actualmente existente em matéria de prova digital, mas que permita também criar as ferramentas necessárias para ultrapassar os obstáculos, ao nível da obtenção de prova, que a criminalidade informática coloca, adaptando o Direito à realidade tecnológica contemporânea.

Pensamos, especificamente, na possibilidade de aceder aos dados contidos num determinado sistema informático, como seja um computador, observá-los e, se necessário, recolhê-los sem o conhecimento do visado. Estas técnicas são, geralmente, associadas à figura do cibercriminoso, mas torna-se cada vez mais importante considerar a sua utilização para fins de investigação criminal. De facto, um dos principais problemas apontados pela Doutrina à Lei do Cibercrime é o facto de o legislador não ter resolvido expressamente o problema da admissibilidade da infiltração electrónica em sistemas informáticos, com vista à obtenção de informações e dados do visado, sem o conhecimento deste. Esta infiltração pode ser feita através da instalação de *malware*[1] nos dispositivos electrónicos do visado, nomeadamente computadores, telemóveis e *tablets*. Assim, o presente estudo centra-se no tema da

[1] Numa primeira abordagem, podemos adiantar que *malware*, termo que resulta do inglês *malicious software* (*software* malicioso), refere-se a qualquer programa informático concebido para infiltração em sistemas de computador alheios, com o intuito de causar danos, alterações ou roubo de informações.

investigação criminal em ambiente digital, nomeadamente sobre a eventual possibilidade de utilização de *malware* como meio oculto de obtenção de prova.

Contudo, não podemos cair no erro de chegar a um regime processual *Orwelliano*. Os meios ocultos de investigação criminal não podem, nunca, tornar-se a regra e não a excepção. Nas palavras de Costa Andrade, "*o que é tecnicamente possível não é, só por si e sem mais, legítimo."*[2] Ainda assim, não se pode negar a necessidade de actualização e ajustamento dos meios de obtenção de prova, no sentido de acompanhar o desenvolvimento técnico, científico e social. Assim, pretendemos com o presente estudo procurar saber se existe já base legal para fundamentar o recurso a *malware* como meio de obtenção de prova e se, por outro lado, é admissível a sua utilização e em que termos à luz dos princípios fundamentais do Estado de Direito Democrático.

[2] ANDRADE, Manuel da Costa, "*Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009, p.150 (itálico nosso)

2. As tecnologias de informação e a investigação criminal

O desenvolvimento das tecnologias de informação[3], nomeadamente do computador e das redes informáticas trouxe importantes modificações ao nível social, económico e cultural. As sociedades modernas encontram-se cada vez mais dependentes da utilização de sistemas informáticos. Grande parte da população tem acesso à *Internet* na palma da mão, através de *smartphones* ou *tablets*[4], podendo aceder, consultar, receber e partilhar conteúdos de qualquer natureza, sem obstáculos temporais ou territoriais. Também as empresas e o próprio Estado têm vindo a utilizar cada vez mais os sistemas de informação e comunicação para gerir o seu funcionamento e para a prestação de serviços essenciais. O ciberespaço é "o epicentro do mercado, o lugar de criação e da aquisição de conhecimentos, o principal meio da comunicação e da vida social."[5]

Não podemos negar que, por um lado, a *Internet*, e outras tecnologias de informação, actualmente desempenham um papel fundamental na nossa sociedade; por outro lado, não podemos também ignorar as vantagens desta realidade. Em primeiro lugar, a desmaterialização de certos serviços do Estado e das empresas, através da informatização, permite racionalizar os mesmos e diminuir custos associados à manutenção daqueles. Por outro lado, em certos casos facilita a vida dos cidadãos, que têm maior facilidade de acesso a determinados serviços, sem implicar deslocações. Por exemplo, o Portal do Cidadão[6] permite fazer *online* o pedido de

[3] "[a] designação T[ecnologias de] I[nformação] conglomera todas as formas de tecnologias destinadas à criação, armazenamento, troca e utilização de informação nos seus diversos formatos, possibilitando a inclusão das tecnologias de computação e de telecomunicações num mesmo conceito, englobando para além do processamento de dados, os sistemas de informação, a engenharia de software e a informática, sem descurar o 'factor humano', questões administrativas e organizacionais." INÁCIO, André, "Tecnologias de Informação e Segurança Pública: Um Equilíbrio Instável", *Revista Científica Sobre Cyberlaw,* CIJC, Faculdade de Direito de Lisboa, n.º 1, Janeiro 2016, p. 61, disponível em http://www.cijic.org/publicacao/

[4] Segundo o Inquérito à Utilização de Tecnologias de Informação e de Comunicação pelas Famílias, realizado pelo INE (2014), em Portugal, entre os utilizadores de *Internet*, mais de metade (57%) acede à *Internet* em mobilidade, isto é, fora de casa e do local de trabalho em equipamentos portáteis (telemóvel, *smartphone*, computador portátil ou outro equipamento portátil), disponível em http://www.ine.pt/

[5] LEVY, Pierre, *A Conexão Planetária,* p.51, *apud* CONTE, Christiany Pegorari e FIORILLO, Celso Antonio Pacheco, *Crimes no Meio Digital*, Editora Saraiva, 2015, p.21

[6] Mais informações em http://www.portaldocidadao.pt/

alteração de morada do cartão do cidadão, o pedido de certificado de admissibilidade de firma ou denominação para efeitos de constituição de sociedade comercial, entre outros.

Além dos serviços do Estado, é possível realizar todo o tipo de operações através da *Internet* - compras *online* em praticamente qualquer loja ou supermercado, comprar bilhetes para espetáculos, fazer reservas em restaurantes, encomendar refeições, consultar saldos e movimentos de contas bancárias, efectuar pagamentos, carregamentos ou transferências, consultar e modificar dados pessoais de determinados serviços (v.g. Via Verde *Online*, onde é possível, entre outras funcionalidades, alterar o nome, a morada ou o número de matrícula da viatura associada ao identificador), entre tantas outras possibilidades.

Além disso, a *Internet* desempenha também um papel fulcral ao nível da cultura e do entretenimento, bem como da interacção social. Veja-se, a título de exemplo, o caso da rede social *Facebook* utilizada por cerca de 1.038 milhões de pessoas, quase 39% da população mundial, sendo que só em Dezembro de 2015, 800 milhões de pessoas utilizaram esta rede social para troca de mensagens.[7]

Se o desenvolvimento das tecnologias de informação veio acompanhado de inúmeras vantagens, a verdade é que também veio facilitar a prática de infracções criminais através dos sistemas informáticos e, nomeadamente, da *Internet*. A Sociedade da Informação é, por defeito, uma sociedade vulnerável.[8] Por um lado, as características do meio informático propiciam e facilitam a actividade delituosa; por outro lado, a actividade de prevenção, investigação e repressão dessa criminalidade tem-se tornado cada vez mais difícil, pelo que vulnerabilidade e a probabilidade de impunidade torna o ambiente informático ainda mais atraente. Torna-se, assim, imprescindível que o Direito Penal e o Direito Processual Penal acompanhem esta evolução tecnológica, que se traduz numa eminente modernização da criminalidade, de forma a garantir uma resposta eficaz aos desafios que esta *sociedade digital* lhes coloca.

[7] Informação disponível em http://bit.ly/1UKBbER

[8] Expressão utilizada por SIEBER, Ulrich, *Legal Aspects of Computer Related Crime in the Information Society – COM-CRIME Study – prepared for the European Commission*, 1998, p.3

3. O ambiente digital

Quando nos referimos a ambiente digital pensamos, sem preocupação de exaustão na conceptualização, no "espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações, [nomeadamente] na *Internet* e nos computadores a ela ligados,"[9] sendo que a *Internet* se apresenta, "[não] como uma entidade física ou tangível, mas configura uma rede de redes interligadas."[10]

3.1. As características

Para melhor compreensão dos problemas que o ambiente digital pode colocar no que diz respeito à investigação criminal, julgamos ser necessário, num primeiro momento, abordar sucintamente os elementos que o caracterizam.

O ambiente digital assume um carácter transnacional ou transfronteiriço, na medida em que a *Internet* permite conectar computadores, ou qualquer outro tipo de sistema informático, localizados em pontos opostos do mundo. É possível realizar comunicações para qualquer parte do mundo, ou aceder a qualquer tipo de informação disponível na rede, independentemente da localização física da sua origem. A noção de espaço físico ou de território perde sentido no ambiente digital, porquanto se trata de uma "realidade virtual, presente ao mesmo tempo em qualquer lugar e em lugar nenhum."[11] A prática de delitos deixa de estar dependente de uma base física de território, deixa de estar limitada pela distância e não conhece fronteiras. Além disso, esta característica determina que um mesmo crime informático possa implicar, pelo menos, dois ordenamentos jurídicos distintos, levando a dificuldades de qualificação do ilícito e de determinação da lei aplicável. Como salientam Celso Fiorillo e Christiany Conte, "um

[9] MOREIRA, João Manuel Dias, "O impacto do ciberespaço como nova dimensão nos conflitos", *Boletim Ensino|Investigação do IESM*, n.º 13, Novembro 2012, p. 30

[10] CONTE, Christiany Pegorari e FIORILLO, Celso Antonio Pacheco, *Crimes no Meio Digital*, Editora Saraiva, 2015, p.160

[11] MOREIRA, João Manuel Dias, "O impacto do ciberespaço como nova dimensão nos conflitos", *Boletim Ensino|Investigação do IESM*, n.º 13, Novembro 2012, p. 31

agente pode estar no Chile e invadir o sistema informático de uma empresa sediada no Canadá, (…) sendo que os prejuízos provocados ocorrerão no Japão."[12]

Mais, o anonimato associado ao meio informático torna-o atractivo para a prática de comportamentos ilícitos. Através da *Internet,* a comunicação e a navegação não envolvem qualquer tipo de contacto pessoal e a identidade dos utilizadores pode ser facilmente falsificada. São enumeras as possibilidades de um utilizador navegar de forma anónima em rede, através, por exemplo da criação de um perfil falso ou a utilização de um endereço electrónico com dados fictícios. Veja-se, a título de exemplo, que cerca de 8,7% dos perfis no *Facebook* são falsos.[13] Existem, ainda, áreas da *Internet* especificamente concebidas para garantir o anonimato dos utilizadores – a chamada *Deep Web,* que se contrapõe à *Surface Web,* esta última sendo aquela *Internet* que todos conhecemos e à qual recorremos no nosso dia-a-dia. Já a *Deep Web* apenas é acessível através da utilização de *softwares* específicos, como o *The Onion Router* ou o *Freenet,* dirigidos à anonimização dos seus utilizadores e dos conteúdos acedidos ou partilhados pelos mesmos.[14]

Além da problemática do anonimato, frequentemente os cibercriminosos detêm elevados conhecimentos informáticos, que permite que recorram, por exemplo, a técnicas de dissimulação de IP[15] para ocultar as suas "*pegadas digitais,*"[16] bem como a mecanismos de

---

[12] CONTE, Christiany Pegorari e FIORILLO, Celso Antonio Pacheco, *Crimes no Meio Digital*, Editora Saraiva, 2015, p.161

[13] CLULEY, Graham, "*Facebook: There are over 83 million fake accounts on our site"*, 2 de Agosto de 2012, disponível em http://bit.ly/1pZoyKO

[14] Maior desenvolvimento sobre a *Deep Web* em RAMALHO, David Silva, "A investigação criminal na *Dark Web*", *Revista de Concorrência e Regulação* Ano IV, n.º 14/15, Abril-Setembro 2013, pp. 387-396.

[15] O endereço IP (*Internet Protocol*) é um número representado no formato decimal como, por exemplo, "192.168.1.3". A primeira parte do endereço identifica uma rede específica na *Internet*, a segunda parte identifica um *host* dentro dessa rede. O endereço IP não identifica uma máquina individual, mas uma conexão à *Internet*. É possível, a partir deste endereço, determinar a localização da máquina ou da origem de determinada mensagem enviada. Existem, contudo, determinadas técnicas que permitem alterar ou esconder o endereço de IP, de forma a impossibilitar a localização e identificação do utilizador. Maior desenvolvimento em http://techterms.com/definition/ipaddress

[16] Expressão utilizada por FACHANA, João, "Reflexões sobre o anonimato no mundo digital", *Linhas Tortas*, Ordem dos Advogados – Conselho Distrital do Porto, Edição n.º 8, Maio de 2013, p.3, disponível em http://bit.ly/1Rhr99C

encriptação e codificação de ficheiros, que tornam as suas informações e comunicações ininteligíveis para terceiros, inviabilizando-se a sua identificação e localização pelas autoridades judiciárias.

3.2.As dificuldades de investigação

As dificuldades de prevenção, investigação, comprovação e punição do cibercrime derivam de todas as características supra enunciadas, tal como já fomos referindo a propósito de cada uma delas. São essas as características que, ao mesmo tempo que facilitam a actividade criminosa em ambiente digital, dificultam também a sua investigação. Além das dificuldades que resultam directamente das características já referidas, existem outros problemas.

Em primeiro lugar, apresenta-se como problemática a falta de legislação nacional adequada em matéria de prova digital. Desde logo, a regulação da prova digital encontra-se espalhada por vários diplomas legais, nomeadamente o Código de Processo Penal, a Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro) e a Lei n.º 32/2008, de 17 de Julho, que diz respeito à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas. Nas palavras de João Conde Correia, "[e]sta trilogia (…) contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático. A prova digital – essencial no mundo hodierno – continua mergulhada num verdadeiro pântano prático, e sobretudo, normativo (…)."[17] De facto, a articulação destas leis levanta problemas, desde logo em saber como conjugar as três e qual o regime processual aplicável que dela resulta, o que se repercute, naturalmente, ao nível da investigação criminal. Por exemplo, actualmente, existem três regimes processuais diferentes de aquisição de dados de base, de tráfego e de localização: o regime que resulta do CPP, o que resulta da Lei n.º 32/2008, de 17 de Julho e o que resulta da Lei do Cibercrime.[18]

---

[17] CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, Ano 35, n.º 139, Julho-Setembro 2014, p. 30

[18] Problemática desenvolvida por PINHO, Carlos, "Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho", *Revista do Ministério Público*, Ano 33, n.º 129, Janeiro-Março 2012, pp. 63-93

Além disso, é também necessário caminhar no sentido da uniformidade legal internacional em matéria de cibercrime, procurando harmonizar os quadros normativos, pois só assim "a cooperação internacional será verdadeiramente eficaz, extinguindo-se os 'paraísos cibernéticos.'"[19] Só a cooperação e coordenação internacional poderá permitir resposta eficaz a ataques cibernéticos, tendo em conta a já referida característica da transnacionalidade.

Por outro lado, é imprescindível a existência de dispositivos processuais, nomeadamente meios de obtenção de prova, especificamente pensados para combater a criminalidade informática. Não obstante a Lei do Cibercrime ter vindo consagrar "um verdadeiro sistema processual de prova digital,"[20] a verdade é que o constante progresso científico deveria ser acompanhado por uma actuação constante do legislador, adaptando os mecanismos de obtenção de prova à realidade tecnológica. Como salienta Armando Dias Ramos, "[o] que vigora entre nós, na Lei do Cibercrime, é decalcado da Convenção do Cibercrime, redigida em 2001. Volvidos mais de 15 anos, a tecnologia evoluiu de forma inimaginável."[21] Recentemente, é de notar que também a Procuradora-Geral da República, Joana Marques Vidal, alertou na conferência "os desafios da criminalidade na *darkweb*", que decorreu no dia 11 de Março de 2016, para a necessidade de, em matéria de cibercrime, "avaliar a suficiência das leis penais existentes e de ponderar uma eventual alteração, caso as existentes não bastem."[22] O criminoso digital, especialmente no âmbito da criminalidade organizada, tem, na maior parte dos casos, elevados conhecimentos informáticos, e mune-se dos mais avançados meios tecnológicos, acompanhando incansavelmente a sua evolução, realidade à qual julgamos que não tem sido dada a devida importância pelo legislador nacional.

Existem já meios técnicos disponíveis, utilizados pela própria criminalidade, que podem auxiliar a investigação criminal, contudo é necessário que sejam legítimos e

[19] DIAS, Vera Marques, "A problemática da investigação do cibercrime", *Data Venia*, Ano 1, n.º1, p.78, disponível em http://www.datavenia.pt/

[20] CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, Ano 35, n.º 139, Julho-Setembro 2014, p. 35

[21] RAMOS, Armando Dias, "A prova digital na investigação do (ciber)terrorismo", *Investigação Criminal* n.º 9, Dezembro de 2015, ASFICPJ, p.133

[22] Cfr. "PGR alerta para eventual necessidade de alterar leis do cibercrime", *JusJornal*, n.º 2336, 14 de Março de 2016, disponível em http://jusjornal.wolterskluwer.pt/

admissíveis, carecendo de previsão e regulação legal expressa. É imperativo colocar as novas tecnologias ao serviço da Justiça, munindo o investigador criminal de ferramentas informáticas que permitam fazer face aos desafios que as particularidades do ambiente informático colocam. É, ainda, fundamental garantir uma adequada formação e treino especializado para os investigadores criminais, que lhes permita adquirir os conhecimentos técnicos e científicos necessários para a utilização destas novas tecnologias para recolha da prova digital, de forma a maximizar a eficácia do seu uso, bem como para garantir a viabilidade da utilização, em julgamento, das provas recolhidas.

4. Os meios ocultos de investigação criminal

Os meios ocultos de investigação caracterizam-se genericamente "pela utilização por parte da entidade investigadora de meios enganosos, dissimulados ou mesmo insidiosos contra a pessoa investigada que, assim (…), age espontaneamente, 'inocentemente', entregando informações e provas aos investigadores, ou praticando actos ilícitos, ou tendencialmente ilícitos, comportamentos esses que não assumiria se tivesse conhecimento do *engano*."[23] No contexto da criminalidade informática, a utilização de meios ocultos tem evidentes vantagens ao nível da descoberta do crime e da obtenção de provas. Pense-se, por exemplo, na iniciativa tomada pela ONG holandesa *Terre des Hommes* para atrair e identificar predadores sexuais infantis na *Internet*. Esta organização criou um modelo animado de uma criança, a Sweetie, que uma equipa utilizou como disfarce para entrar em fóruns *online.* No período de dez semanas, mais de vinte mil homens abordaram a "criança" e cerca de mil estavam dispostos a pagar para a verem em actos sexuais através da *webcam.*[24] Pense-se, ainda, na operação levada a cabo pelo grupo *Anonymous*[25]*,* finda a qual foi publicada uma lista com informação pessoal

[23] COSTA, Eduardo Maia, "Acções Encobertas (Alguns Problemas, Algumas Sugestões)," *Estudos em Memória do Conselheiro Artur Maurício*, Coimbra Editora, 2014, p. 357

[24] SOARES, Maria, "Sweetie, a menina virtual que ajudou a encontrar predadores sexuais na *Internet*", *Público,* 5 de Novembro de 2013, disponível em http://bit.ly/1ZnrjSa

[25] Grupo de activistas na *Internet*; apesar de não terem nenhuma ideologia formalmente definida, são conhecidos por utilizar os seus conhecimentos informáticos para promover a liberdade de expressão e os direitos humanos. Recentemente, em Novembro de 2015, no seguimento dos ataques terroristas em Paris, o grupo reagiu publicamente, declarando que iria iniciar uma operação contra o grupo Estado Islâmico do Iraque e do Levante (conhecido por ISIS), com o objectivo de encontrar os seus membros e fazer cessar as suas actividades na *Internet* Cfr. http://bit.ly/1J9tdzp

dos utilizadores de *websites* de pornografia infantil, nomeadamente os seus nomes, profissões, localização, endereço IP, entre outras. [26]

É entendimento dominante que os meios ocultos de investigação "vieram para ficar."[27] Aliás, são cada vez mais encarados como verdadeiramente imprescindíveis para a perseguição e repressão criminal, especialmente no que diz respeito às modernas formas de criminalidade. Contudo, e como tem sido apontado pela doutrina, não é possível encontrar entre todos os meios ocultos de investigação um sistema equilibrado, pelo que o direito português dos meios ocultos se caracteriza "pelas lacunas e descontinuidades, incongruências e inconsistências e, sobretudo, por insustentáveis contradições e assimetrias normativas axiológicas e político-criminais."[28] De facto, enquanto uns meios ocultos estão regulados no CPP, nomeadamente as escutas telefónicas, a maioria deles encontra-se disperso por diplomas extravagantes, revelando assim "a parcimónia e a incomodidade do legislador"[29] em admiti-los. Pense-se no caso das acções encobertas (Lei n.º 101/2001, de 25 de Agosto), da videovigilância (Lei n.º 1/2005, de 10 de Janeiro), dos exames de ADN (Lei n.º 5/2008, de 12 de Fevereiro), entre tantos outros.

Não pretendemos negar a importância dos meios ocultos de investigação, tanto mais que nos dedicamos precisamente ao estudo de um. Contudo, é necessário, por um lado, garantir que a sua utilização se mantém excepcional e conforme às exigências constitucionais em matéria de restrição de direitos fundamentais; por outro lado, julgamos afigurar-se da maior importância caminhar no sentido de alcançar um "verdadeiro sistema global e unificado, pelo menos em sede de pressupostos ou requisitos da sua admissibilidade,"[30] sugerindo-se na doutrina o seu completo reagrupamento no CPP, à semelhança do que acontece na Alemanha.[31]

---

[26] GALLAGHER, Sean, "Anonymous takes down darknet child porn site on Tor network", *Ars Technica*, 24 de Outubro de 2011 – notícia completa em http://bit.ly/1LDjyoZ

[27] ANDRADE, Manuel da Costa, "*Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009, p.106

[28] *Idem* p.109

[29] COSTA, Eduardo Maia, "Acções encobertas (Alguns problemas, algumas sugestões), *Estudos em emória do Conselheiro Artur Maurício,* Coimbra Editora, 2014, p. 359

[30] RODRIGUES, Benjamim Silva, *As Novas Fronteiras do Direito no Dealbar do Século XXI*, Rei dos Livros, 2012, p. 22

[31] Cfr. ANDRADE, Manuel da Costa, "*Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009, p.109 e

Um dos meios ocultos de investigação criminal que tem vindo a chamar a atenção da doutrina é a possibilidade de aceder remotamente aos dados contidos em dispositivos electrónicos, monitoriza-los e recolhê-los sem o conhecimento do visado, habitualmente denominado pela doutrina como "busca *online*", ao qual nos dedicaremos de seguida.

5. Malware – conceito e modalidades

5.1. Precisão terminológica: *malware* ou buscas *online*?

A maioria da Doutrina refere-se à infiltração em sistemas informáticos como "busca *online,*" não obstante haver já alguma concordância quanto à imprecisão do termo. Costa Andrade reconhece que se trata de "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 actualizam na observação, busca, cópia, vigilância, etc., dos dados presentes naqueles sistemas informáticos."[32] Também Benjamim Silva Rodrigues entende que este meio oculto de investigação é de forma imprópria reconduzida à denominada "busca *online.*"[33] Ainda, David Silva Ramalho entende, especificamente em relação à utilização de *malware*, que "se trata de um conceito novo no plano jurídico e que merce destacamento de outros conceitos com contornos e propósitos diferentes." [34]

Ainda que seja possível adaptar o conceito tradicional de busca[35], julgamos, na esteira do defendido por David Silva Ramalho, ser pertinente tratar a questão com referência à

RODRIGUES, Benjamim Silva, *As Novas Fronteiras do Direito no Dealbar do Século XXI*, Rei dos Livros, 2012, p.22

[32] ANDRADE, Manuel da Costa, "*Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009, p.166 (itálico nosso)

[33] RODRIGUES, Benjamim Silva, Da Prova Penal – Tomo II – *Bruscamente… A(s) face(s) oculta(s) dos métodos ocultos de investigação criminal*, Rei dos Livros, 1ª edição, 2010, p. 471

[34] RAMALHO, David Silva, "O uso de *malware* como meio de obtenção de prova em processo penal" *Revista de Concorrência e Regulação*, Ano IV, n.º 16, Outubro-Dezembro 2013, p. 199

[35] "As buscas são levadas a cabo em lugar reservado ou não livremente acessível ao público, quando houver indícios de que nesses locais se esconde o arguido (…) ou que neles se encontram quaisquer objectos relacionados

utilização de *malware,* que porventura permite abarcar uma realidade mais ampla de situações, sem deixar de incluir as situações que a doutrina tem referido como sendo buscas *online.* A título de exemplo, Paulo Pinto de Albuquerque, definindo busca *online* como "a infiltração electrónica em sistemas informáticos, por exemplo, através dos chamados cavalos de Tróia, de modo a que o investigador possa em tempo real ou deferido conhecer a informação que está a ser introduzida ou já foi introduzida no sistema, incluindo textos, sons e imagens"[36], faz referência expressa a um tipo de *malware* – Cavalo de Tróia. Julgamos, contudo, que o conceito de busca já não permite abarcar as situações em que a utilização de *malware* se traduz, por exemplo, na observação oculta da actividade que o utilizador desenvolve no sistema informático ou, através dele, na *Internet*.[37] Assim, julgamos ser pertinente, no contexto do presente estudo, a autonomização dos conceitos.

5.2. O conceito de *malware*

O *malware* pode ser definido como "um programa que discretamente se instala num sistema de processamento de dados, sem o conhecimento ou consentimento do utilizador, com o objectivo de colocar em perigo a confidencialidade dos dados, a integridade dos dados [ou] a disponibilidade do sistema."[38] Assim, a utilização de *malware* enquanto meio de obtenção de prova consiste, essencialmente, na infiltração em determinado sistema informático (v.g. um computador), com a particularidade de que o visado pode nunca chegar a ter conhecimento dessa intromissão. Sem prejuízo dos diversos tipos de modalidades de *malware*, às quais faremos referência infra, a sua utilização possibilita, genericamente, a observação e vigilância em tempo real e a cópia dos dados presentes no sistema informático em causa. É também

---

com um crime ou que possam servir de prova no processo em curso. A busca visa, pois, a detenção do arguido (…) ou a descoberta de objectos relacionados com um crime ou que possam servir de prova no processo. – Cfr. JESUS, Francisco Marcolino, *Os Meios de Obtenção de Prova em Processo Penal*, Almedina, 2.ª edição, 2015, p.226

[36] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 2011, p. 502

[37] Parece ser do mesmo entendimento Rita Castanheira Neves, distinguindo entre busca *online* e "vigilância oculta do visado na *Internet.*" Cfr. *As Ingerências nas Comunicações Electrónicas no Processo Penal*, Coimbra Editora, 2011, p.201

[38] FILIOL, Eric, *Computer viruses: from theory to application*, Springer, 2005, p. 83

possível, através da instalação de *malware*, activar remotamente a câmara e o microfone do aparelho electrónico infectado.

5.3. Algumas modalidades de *malware*[39]

Sem prejuízo da existência de outros tipos de *malware*, faremos aqui uma breve síntese daqueles que nos parecem mais relevantes neste contexto, tendo em conta as suas características e modo de funcionamento.

Começamos pelos Cavalos de Tróia, porventura a modalidade mais conhecida, que podem ser definidos como um tipo de *malware* que se apresenta, na maioria dos casos, como um ficheiro ou um *website* inofensivo, levando a que o próprio utilizador visado active as suas funcionalidades, descarregando o anexo de uma mensagem de correio electrónico, abrindo determinada página da *Internet* infectada com código malicioso ou através da instalação de falsas actualizações de *software* legítimo.[40] Este tipo de *malware* tende a ser utilizado para criar formas ocultas de aceder remotamente ao sistema informático (chamadas *backdoors*), sem o conhecimento do utilizador. Através do acesso propiciado pelo cavalo de Tróia, é possível apagar, alterar ou copiar ficheiros do computador infectado, recolher credenciais de acesso e outras informações confidenciais, desactivar ou activar *hardware* (como o teclado, o rato, a câmara e o microfone), desactivar programas antivírus e de detecção de *malware*, executar comandos, além de ser possível, em geral, monitorizar toda a actividade desenvolvida pelo utilizador do computador infectado.[41]

O *spyware* consiste num programa informático que recolhe informação sobre uma pessoa ou organização sem o seu conhecimento ou consentimento.[42] Este tipo de *malware* permite obter informações pessoais, como nomes, moradas ou listas de *websites* visitados,

---

[39] Para maior desenvolvimento sobre cada modalidade de *malware* e seu funcionamento recomendamos o estudo de RAMALHO, David Silva, "O uso de *malware* como meio de obtenção de prova em processo penal" *Revista de Concorrência e Regulação,* Ano IV, n.º 16, Outubro-Dezembro 2013, pp. 199 - 207

[40] Cfr. *Idem* p. 203

[41] ERBSCHLEO, Michael, *Trojans, Worms and Spyware – A Computer Security Professional's Guide to Malicious Code*, Elsevier Butterworth–Heinemann, 2005, p.22

[42] *Idem* p.25

podendo ainda incluir *keyloggers,* que permitem gravar informação sobre as teclas premidas pelo utilizador, de forma a obter nomes de utilizador e respectivas palavras-passe ou números de cartão de crédito, entre outros.[43] Na maior parte dos casos, os programas de s*pyware* têm a capacidade de proceder à sua actualização autonomamente ou descarregar automaticamente novas versões, o que permite introduzir novas funções e evita também a sua detecção por programas anti-vírus ou anti-*spyware*.[44]

Os *rootkits*, por sua vez permitem obter remotamente acesso exclusivo a um sistema informático, em regra obtendo o acesso equivalente ao de administrador, "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.*"[45]

As *logic bombs* são um tipo de *malware* que se instala num sistema informático e que se mantém inactivo, aguardando determinado evento que funciona como mecanismo de desencadeamento (pode ser uma data ou uma hora específica ou determinado comando do utilizador do dispositivo infectado, tal como apagar determinados ficheiros) dos seus efeitos nocivos no sistema infectado.[46] É comum ser referido o caso de um administrador da rede informática de uma empresa que, depois de ter sido despedido, nela instalou uma *logic bomb*, programada para se activar e cifrar todos os documentos da empresa quando o seu nome fosse apagado do registo de contabilidade; quando esse evento se verificou, todos os documentos da empresa foram cifrados por uma chave secreta aleatória, que nem próprio o administrador conhecia, tornando praticamente impossível recuperar os documentos perdidos.[47]

O vírus é um tipo de *malware* concebido para se replicar e espalhar no sistema informático (v.g. computador), podendo danificar o sistema, eliminar dados e desactivar

---

[43] FILIOL, Eric, *Computer viruses: from theory to application*s, Springer, 2005, p.328

[44] BOLDT, Martin, *Privacy-Invasive Software,* Blekinge Institute of Technology, 2010 p. 75

[45] RAMALHO, David Silva, "O uso de *malware* como meio de obtenção de prova", *Revista de Concorrência e Regulação*, Ano IV, n.º 16, Outubro-Dezembro 2013, p.204

[46] *Ibidem*

[47] FILIOL, Eric, *Computer viruses: from theory to application*s, Springer, 2005, p.120

programas de segurança (por exemplo, os programas anti-vírus).[48] O vírus, em regra, necessita de interacção humana para se propagar, nomeadamente através da utilização de um CD-ROM ou de um suporte USB. Já os *worms* são muito similares aos vírus no que diz respeito aos seus efeitos práticos, mas propagam-se pela internet, não dependendo de interacção humana.[49]

5.4.A utilização de *malware* na lei portuguesa – da inexistência de regimes aplicáveis

É unânime na doutrina, como veremos infra, que a lei portuguesa não prevê expressamente a possibilidade de recurso à intromissão oculta em sistemas informáticos. Contudo, alguns autores avançam a possibilidade de aplicação de outros regimes, que julgamos ser pertinente sumariamente referir, de forma a averiguar se podemos, efectivamente, encontrar uma base legal no ordenamento jurídico português que permita sustentar a utilização de *malware* como meio de obtenção de prova.

Paulo Pinto de Albuquerque entende que este meio de obtenção de prova veio ser consagrado no artigo 15.º da LC, que prevê a *"pesquisa em sistema informático",* concluindo, contudo, pela sua inconstitucionalidade por intrusão na privacidade manifestamente desproporcional, "na medida em que a lei não coloca restrições relativamente ao conteúdo dos dados que podem ser pesquisados e, além disso, permite que o MP e o OPC ordenem a pesquisa de um sistema informático (…) sem o controlo prévio ou posterior da 'pesquisa' por um juiz."[50]

Já Rita Castanheira Neves entende que a lei não oferece solução para a possibilidade de poderem ser recolhidos dados informáticos sem o conhecimento do visado, na medida em que "[a] referência à presença da autoridade judiciária na diligência de pesquisa de dados informáticos no n.º1 do artigo 15.º, bem como o elenco das formas de apreensão dos dados informáticos nas alíneas a) a d) do n.º7 do artigo 16.º da Lei do Cibercrime, deixam de foram

[48] ERBSCHLEO, Michael, *Trojans, Worms and Spyware – A Computer Security Professional's Guide to Malicious Code*, Elsevier Butterworth–Heinemann, 2005, p.19

[49] BOLDT, Martin, *Privacy-Invasive Software,* Blekinge Institute of Technology, 2010 p. 11

[50] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 2011, p. 502

a possibilidade de as instâncias formais de controlo poderem levar a cabo buscas sem que o visado seja directamente confrontado com a diligência."[51]

Do mesmo modo, João Conde Correia, entendendo que a lei não oferece solução expressa, apresenta duas interpretações possíveis. Por um lado, poderá entender-se, na esteira de Paulo Pinto de Albuquerque, que as buscas *online* estão consagradas no artigo 15.º n.º 5 da LC. Contudo, "o que está aqui em causa é apenas a extensão online de uma pesquisa de dados informáticos em curso. Não se trata, pois, de uma diligência complementarmente oculta, realizada à revelia do visado."[52] Por outro lado, a referência a *"meios dispositivos e informáticos"* do artigo 19.º n.º 2 da LC poderá ser interpretada como prevendo a possibilidade de realizar buscas *online*, possibilidade esta limitada, contudo, ao contexto das acções encobertas.

David Silva Ramalho entende que resulta do artigo 19.º n.º 2 da LC a consagração de um novo meio oculto de obtenção de prova – a utilização de *malware* – com a sua utilização limitada ao contexto excepcional das acções encobertas, por força da sua inserção sistemática. Entende o Autor que esta interpretação resulta do facto de os "*meios e dispositivos informáticos*" a que o artigo alude não se subsumirem a qualquer um dos meios de obtenção de prova previstos na legislação portuguesa, de onde deriva a intenção do legislador de legitimar o recurso a um novo meio de obtenção de prova.[53] Conclui, contudo, pela inconstitucionalidade por violação conjugada dos artigos 18.º n.º 2, 26.º n.º 2 e 32.º n.º 1 e 5 da CRP.

Por outro lado, de acordo com o relatado por David Silva Ramalho, os membros de órgãos de polícia criminal têm vindo a sugerir a aplicação directa do regime da intercepção de comunicações, previsto no artigo 18.º da LC[54], que remete para a aplicação do regime da

---

[51] NEVES, Rita Castanheira, *As Ingerências nas Comunicações Electrónicas em Processo Penal,* Coimbra Editora, 2011, p. 284

[52] CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público,* Ano 35, n.º 139, Julho-Setembro 2014, p. 42

[53] Maior desenvolvimento em RAMALHO, David Silva, "O uso de *malware* como meio de obtenção de prova em processo penal" *Revista de Concorrência e Regulação*, Ano IV, n.º 16, Outubro-Dezembro 2013, pp. 229-233

[54] Cfr. *Idem* p. 226

intercepção e gravação de conversações ou comunicações telefónicas constantes dos artigos 187.º, 188.º e 190.º do CPP.

Quanto a nós, em primeiro lugar, também não concordamos com aplicação do artigo 19.º n.º 2 da LC, na medida em que a formulação do mesmo é demasiado vaga[55] para poder sustentar a consagração de um novo meio de obtenção de prova, especialmente estando em causa um meio oculto. Tratando-se de um meio de obtenção de prova susceptível de constituir uma restrição de direitos fundamentais, terá necessariamente que ter consagração legal expressa e especifica prevendo "a medida de compressão dos direitos fundamentais, fixar a sua compreensão, extensão (…) bem como definir os seus limites."[56] A não ser assim, só podemos, tal como David Silva Ramalho, concluir pela sua inconstitucionalidade.

No que diz respeito à aplicação do artigo 18.º da LC, julgamos, tal como parece ser o entendimento dominante[57], que o que está em causa não é a intercepção de comunicações, isto é, "a intercepção de mensagens de correio electrónico em tempo real, ou seja, no seu trajecto do computador do emissor para o computador do receptor através da rede de servidores. Ou ainda a intercepção de mensagens trocadas através de processos de comunicações instantânea (usualmente designados por serviços de 'Chat.)."[58] Aquilo que se pretende com a instalação de *malware* é, entre outras possibilidades, a recolha de dados e/ou monotorização dos dados e da

[55] Artigo 19.º n.º 2 da LC: sendo necessário o recurso a meios e dispositivos informáticos, observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.

[56] ANDRADE, Manuel da Costa, "Métodos ocultos de investigação – *pläydoer* para uma teoria geral", *Que Futuro Para o Processo Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias por Ocasião dos 20 anos do Código de Processo Penal Português,* Coimbra Editora, 2009, p. 541

[57] Neste sentido RAMALHO, David Silva, "O uso de *malware* como meio de obtenção de prova em processo penal" *Revista de Concorrência e Regulação*, Ano IV, n.º 16, Outubro-Dezembro 2013, pp. 226-227; ANDRADE, Manuel da Costa, *"Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009, p. 168; NEVES, Rita Castanheira, *As Ingerências nas Comunicações Electrónicas,* Coimbra Editora, 2011, p. 299

[58] VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada,* Coimbra Editora, 2010, p.119

actividade desenvolvida no computador do visado, pelo que é de concluir pela inaplicabilidade deste regime.[59]

Por outro lado, é também de excluir a aplicação do artigo 15.º da LC. Em primeiro lugar, o n.º 1 deste artigo refere-se a "*dados informáticos específicos e determinados*." Como já tivemos a oportunidade de referir, a utilização de programas de *malware,* pela sua natureza, pode não se cingir sempre à apreensão de dados concretos previamente determinados, visando antes a vigilância das actividades desenvolvidas no sistema informático em causa e a obtenção de dados informáticos respeitantes ao seu utilizador e às suas actividades.

Em relação ao n.º 5 ainda do artigo 15.º, cumpre salientar que a instalação de *malware* não se traduz num caso em que "*no decurso da pesquisa, os órgãos de polícia, executores da medida, nutram a convicção de que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial (...).*"[60] Ou seja, o acesso ao segundo sistema informático tem de ser feito através do primeiro sistema pesquisado, havendo tão só uma extensão da busca inicial, mas esta ainda se incluindo dentro dos parâmetros estabelecidos no n.º1, de onde resulta que a pesquisa não pode ser feita a partir de um outro qualquer sistema informático utilizador pelo investigador.[61] Conclui-se, então, que não é aqui enquadrável a possibilidade de infiltração em sistema informático sem o conhecimento do visado.

Note-se ainda que, na esteira do defendido por Paulo Sousa Mendes, não obstante a lei processual penal estabelecer um regime de prova livre no artigo 125.º, i.e., a não taxatividade dos meios de prova, a verdade é que esta regra não permite que, recorrendo aos meios de prova típicos, sejam criados meios de prova aparentados, mas atípicos. Ou seja, "a liberdade de prova respeita apenas a meios de prova não previstos e não pode significar liberdade relativamente

---

[59] No mesmo sentido ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem,* Universidade Católica Editora, 2011, p.545

[60] RODRIGUES, Benjamim Silva, Da Prova Penal – Tomo IV – *Da Prova Electrónico-Digital e da Criminalidade Informático-Digital,* Rei dos Livros, 2011, p. 528

[61] Cfr. RAMALHO, David Silva, "O uso de *malware* como meio de obtenção de prova em processo penal", *Revista de Concorrência e Regulação,* Ano IV, n.º 16, Outubro-Dezembro 2013, p. 229

aos meios já disciplinados."[62] Assim, concluindo pela inexistência de previsão expressa da utilização de *malware*, ou mesmo da busca *online*, seria sempre de concluir pela sua inadmissibilidade através da tentativa de "encaixe" num outro meio de prova típico.

Mais, conforme resulta do disposto no artigo 18.º n.º 2 da Constituição da República, em matéria de restrição de direitos, liberdades e garantias aplica-se o princípio da reserva de lei – assim, na ausência de lei expressa que autorize o recurso a *malware*, ou mesmo às buscas *online*, não podemos deixar de concluir pela inconstitucionalidade da sua utilização.

6. A utilização de *malware* como meio oculto de obtenção de prova em ambiente digital

A utilização de *malware* como meio de obtenção de prova, apesar da sua especial apetência para combater a criminalidade informática, não deixa de ser altamente intrusiva. Não descurando a crescente importância da prevenção criminal, não podemos também ignorar a "patente danosidade social, expressa no sacrifico de bens jurídicos e direitos fundamentais"[63] que a utilização deste meio acarreta, podendo lesar gravemente os direitos fundamentais do arguido, nomeadamente o direito à reserva da intimidade privada. Além disso, de um ponto de vista processual, este meio de obtenção de prova pode conflituar directamente com as garantias processuais do arguido, nomeadamente o princípio *nemo tenetur se ipsum accusare*, nas suas duas vertentes, nomeadamente o direito ao silêncio e o direito a não facultar meios de prova.

6.1. A utilização de *malware* e o princípio da legalidade da prova

O artigo 125.º do CPP estabelece o princípio da legalidade da prova, ao qual já fizemos uma breve referência, segundo o qual são admissíveis todas as provas que não forem proibidas por lei. Assim, consagra-se a regra da não taxatividade dos meios de prova, instituindo-se um sistema de prova livre ou de liberdade de prova. Não é, portanto, necessário que um meio de prova esteja expressamente previsto para que seja admissível.

---

[62] MENDES, Paulo Sousa, *Lições de Direito Processual Penal*, Almedina, 2013, p.174

[63] ANDRADE, Manuel da Costa, "Métodos ocultos de investigação – *pläydoer* para uma teoria geral", *Que Futuro Para o Processo Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias por Ocasião dos 20 anos do Código de Processo Penal Português,* Coimbra Editora, 2009, p. 536

Os meios de prova atípicos estão, naturalmente, subordinados aos limites constitucionais e legais de admissibilidade de prova. Os primeiros resultam do artigo 32.º n.º 8 da CRP, onde se estabelece a nulidade das provas obtidas sob tortura ou coacção, obtidas com ofensa da integridade pessoal, da reserva da intimidade da vida priva, da inviolabilidade do domicílio e da correspondência ou das telecomunicações. Os limites legais, conformando o disposto na Constituição, resultam do artigo 126.º do CPP.

O artigo 126.º n.^{os} 1 e 2 disciplina as provas absolutamente proibidas, isto é, as provas obtidas mediante tortura, coacção e ofensa da integridade física ou moral da pessoa, que nunca podem ser utilizadas por dizerem respeito a direitos que a Constituição consagra como invioláveis no seu artigo 25.º.

Por outro lado, o n.º 3 disciplina as provas relativamente proibidas, que dizem respeito a direitos que a Constituição admite serem limitados nos casos previstos na lei (artigos 26.º e 34.º n.º 3 e 4 CRP). Esta relatividade da proibição resulta directamente da Constituição quando na segunda parte do n.º 8 do artigo 32.º determina a nulidade das provas obtidas mediante intromissão *abusiva* na vida privada, no domicílio, na correspondência ou nas telecomunicações, devendo-se ter por abusiva a intromissão quando efectuada fora dos casos previstos na lei e sem intervenção judicial ou quando em violação do princípio da proporcionalidade (18.º n.º 2 CRP). Admite-se, assim, "a compressão de direitos constitucionais, numa lógica de proporcionalidade e exigido pelo próprio interesse do Estado no funcionamento da justiça penal."[64]

Contudo, seguindo o entendimento de Paulo Pinto de Albuquerque, "quando o meio de obtenção de prova implicar um elevado grau de intrusão na privacidade do suspeito, ele deve ser previsto por uma lei expressa, salvo consentimento expresso e informado do visado."[65]

Neste caso, como tivemos já oportunidade de referir, estamos perante um meio oculto de investigação que, por definição, independentemente da sua maior ou menor gravidade,

[64] Acórdão do Supremo Tribunal de Justiça de 3 de Março de 2010, proc. n.º 886/07.8PSLSB.L1.S1

[65] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 2011, p. 332

implica sempre uma intrusão na privacidade. Além disso, tratando-se de um meio oculto, a questão do consentimento também não é aplicável a este caso.

6.2.A utilização de *malware* e o direito fundamental à reserva da intimidade da priva privada

Partimos da análise do direito fundamental à reserva da intimidade da vida privada, na medida em que julgamos ser neste domínio que maiores problemas se levantam no que diz respeito à utilização de *malware* como meio de obtenção de prova.

Ao nível internacional este direito vem consagrado no artigo 12.º da Declaração Universal dos Direitos do Homem, no artigo 8.º da Convenção Europeia dos Direitos do Homem, bem como no artigo 17.º do Pacto Internacional de Direitos Políticos e Civis. No ordenamento jurídico português, este direito é tutelado a nível constitucional, no artigo 26.º n.º 1 da CRP. Alguns outros direitos fundamentais funcionam como garantia deste, nomeadamente o direito à inviolabilidade do domicílio e da correspondência (artigo 34.º) e da proibição de tratamento informático de dados referentes à vida privada (artigo 35.º n.º 3).

A Constituição incumbe a lei de estabelecer garantias efectivas para a protecção deste direito (artigo 26.º n.º 2). Revela-se, contudo, tarefa da maior complexidade delimitar o âmbito de protecção da norma, nomeadamente saber aquilo que concretamente se deve entender por vida privada e quais os seus limites ou a sua extensão.

Alguma doutrina e jurisprudência recorre à teoria das três esferas, desenvolvida sobretudo pelo Tribunal Constitucional Alemão, distinguindo três áreas da vida: a vida íntima, a vida privada e a vida pública. A primeira diz respeito àqueles aspectos da vida que devem ser protegidos em absoluto, não se admitindo qualquer intromissão das autoridades ou dos particulares, nem qualquer juízo de proporcionalidade. A segunda área, dizendo respeito à vida privada simples[66], apenas relativamente protegida, englobando "os acontecimentos que cada

[66] Expressão de CANOTILHO, Gomes J.J. e MOREIRA, Vital, *Constituição da República Portuguesa Anotada,* Volume I, Coimbra Editora, 2007, p.468

indivíduo partilha com um número restrito de pessoas".[67] Aqui, "o seu sacrifício em sede de prova em processo penal estará, por isso, legitimado sempre que necessário e adequado à salvaguarda de interesses ou valores superiores, respeitadas as exigências do princípio da proporcionalidade."[68] Por fim, a última área correspondente à dimensão pública da pessoa enquanto parte da vida em comunidade, subtraída ao domínio da publicidade, mas de normal conhecimento por parte de terceiros,[69] tal como a vida profissional.

Paulo Mota Pinto não segue esta teoria, partindo antes da contraposição entre vida privada e vida pública, no sentido em que esta será "a vida social, mundana do indivíduo, enquanto a vida privada é a sua vida particular e pessoal."[70] Januário Gomes, partindo também desta distinção, entende que vida privada será a vida íntima do individuo, compreendendo todos aqueles actos que "não sendo secretos em si mesmos, devem subtrair-se à curiosidade pública (…), como os sentimentos e afectos familiares, os costumes da vida e as vulgares práticas quotidianas."[71]

O Tribunal Constitucional também já por múltiplas vezes se pronunciou sobre o conteúdo da reserva da intimidade da vida privada, cabendo dar destaque à noção adoptada no Acórdão n.º 128/92: "o direito de cada um ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias. (…) neste âmbito privado ou de intimidade está englobada a vida pessoal, a vida familiar, a relação com outras esferas de privacidade (v.g. a amizade), o lugar próprio da vida pessoal e familiar (v.g. o lar ou o domicílio), e bem assim os meios de expressão e comunicação privados (a correspondência, o telefone, as conversas orais, etc)."

---

[67] CABRAL, Rita Amaral, "O direito à intimidade da vida privada (breve reflexão acerca do artigo 80.º do Código Civil)", *Estudos em Memória do Professor Doutor Paulo Cunha,* Faculdade de Direito de Lisboa, 1989, p. 398

[68] ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal,* Coimbra Editora, 1992, p.95

[69] Cfr. ANDRADE, Manuel da Costa, Anotação ao artigo 192.º do Código Penal, *Comentário Conimbricense do Código Penal - Parte Especial*, dirigido por Jorge de Figueiredo Dias, Coimbra Editora, 2012, p.1049

[70] PINTO, Paulo Mota, "O direito à reserva da intimidade da vida privada", *Boletim da Faculdade de Direito,* Volume LXIX, Coimbra, 1993, p.526

[71] GOMES, Januário, "O problema da salvaguarda da privacidade antes e depois do computador", *Boletim do Ministério da Justiça*, n.º 319, Outubro 1982, p.30

Não pretendemos, com o presente estudo, procurar uma densificação exaustiva daquilo que se deve entender por vida privada. Parece-nos consensual, independentemente da teoria concretamente adoptada, que a sua definição parte sempre de uma distinção entre uma área nuclear da privacidade absolutamente inviolável e uma outra área, ainda que privada, já susceptível de ser restringida, com observação dos limites decorrentes da dignidade da pessoa humana e do respeito pelas exigências do princípio da proporcionalidade. Nas palavras de Costa Andrade, "as diferenças no plano semântico não parecem impedir uma significativa sinonímia de fundo."[72] Será, contudo, sempre um conceito de conteúdo variável, na medida em que a sua extensão e, portanto, o seu grau e âmbito de protecção serão sempre mutáveis, "resultante de se tratar de um *conceito cultural*, que varia com o tempo, o espaço, o tipo de pessoas em causa."[73]

Aquilo que actualmente se entende por vida privada é necessariamente diferente daquilo que se entendia há, por exemplo, 50 anos atrás. A ideia de vida privada tem que se adaptar à realidade do momento em que se procura defini-la, tornando-se tanto mais difícil quanto mais evolui a sociedade. Como questiona Januário Gomes, "como edificar um direito à privacidade se as técnicas de captação e armazenamento das informações estão desenvolvidíssimas, se a pessoas se acotovelam na rua, se comprimem nos transportes e, se, sem fazer por isso, se apercebem dos movimentos do vizinho do andar de cima ou do lado?"[74] E cada vez mais é assim, com a utilização constante da *Internet* e, em especial, das redes sociais (v.g. *Facebook, Instagram, Twitter*), através das quais é possível saber (quase) tudo acerca da vida pessoal dos cidadãos, as bases de dados pessoais criadas pelas empresas e pelo Estado, a informatização de praticamente todos os aspectos da vida. Concordamos, por isso, com Gomes Canotilho e Vital Moreira, na medida em que o conceito de esfera privada terá sempre de ser "culturalmente adequado à vida contemporânea."[75]

---

[72] ANDRADE, Manuel da Costa, Anotação ao artigo 192.º do Código Penal, *Comentário Conimbricense do Código Penal - Parte Especial*, dirigido por Jorge de Figueiredo Dias, Coimbra Editora, 2012, p.1049

[73] DIAS, Figueiredo Jorge de, "Direito à informação, protecção da intimidade e autoridades administrativas independentes", *Estudos em Homenagem ao Professor Doutor Sérgio Soares,* Coimbra Editora, 2001, p.627

[74] GOMES, Januário, "O problema da salvaguarda da privacidade antes e depois do computador", *Boletim do Ministério da Justiça*, n.º 319, Outubro 1982, p.32

[75] CANOTILHO, Gomes J.J.; MOREIRA, Vital, *Constituição da República Portuguesa Anotada,* Volume I, Coimbra Editora, 2007, p.468

Neste contexto de constante progresso tecnológico e aparente diminuição do espaço individual e pessoal de cada um, é necessária uma acentuada preocupação em preservar a privacidade dos cidadãos. A possibilidade de ofensa do direito à reserva da intimidade da vida privada aumenta exponencialmente com o desenvolvimento tecnológico, porquanto este último facilita a recolha, armazenamento e tratamento de dados pessoais, facilitando ainda o acesso a esses dados por terceiros. [76]

6.3. A utilização de *malware* e o direito fundamental à inviolabilidade do domicílio

O direito fundamental à inviolabilidade do domicílio e da correspondência (e de outros meios de comunicação privada), como tivemos oportunidade de referir supra, está consagrado no artigo 34.º da CRP e funciona como garantia do direito à reserva da intimidade da vida privada, entendendo-se aqui por domicílio "aquela área que tem por objecto a habitação humana, aquele espaço fechado e vedado a estranhos, onde recatada e livremente se desenvolve toda uma série de condutas e procedimentos característicos da vida privada e familiar, ou seja, um núcleo restrito sob o signo da intimidade, de protecção da vida privada, da liberdade e da segurança individual, onde se desenrola a vivência essencial, no aspecto existencial, da pessoa."[77]

Além da possibilidade de violação da privacidade, a utilização de *malware* é, ainda, susceptível de violar este direito, na medida em que certas modalidades daquela utilização permitem activar a câmara ou o microfone do sistema informático visado. Como salientam Gomes Canotilho e Vital Moreira, "o domicílio não é violado somente quando se entra na morada de alguém sem o seu consentimento. Os modernos meios técnicos possibilitam a invasão do domicílio mediante meios electrónicos, que, além disso, permitem também a devassa das conversas e da vida privada dos moradores. A inviolabilidade do domicílio é seguramente incompatível com tais mecanismos."[78] No mesmo sentido, Costa Andrade, julgando aliás ser consensual o entendimento de que se se reconduzem a violações da

[76] Cfr. DIAS, Figueiredo Jorge de, "Direito à informação, protecção da intimidade e autoridades administrativas independentes", *Estudos em Homenagem ao Professor Doutor Sérgio Soares,* Coimbra Editora, 2001, p.635

[77] Cfr. Acórdão do Supremo Tribunal de Justiça, de 20 de Setembro de 2009, proc. n.º 06P2321

[78] CANOTILHO, Gomes J.J.; MOREIRA, Vital, *Constituição da República Portuguesa Anotada,* Volume I, Coimbra Editora, 2007, p.540

inviolabilidade do domicílio aquelas situações que se reconduzem à "activação através da *Internet* da câmara ou do microfone de computador situado em casa e, por essa via, escutando e observando pessoas ou eventos que ocorrem no interior da habitação."[79]

Ou seja, se através da utilização de *malware* se activar a câmara ou o microfone do computador infectado e este último se encontrar na habitação do suspeito ou arguido, teremos uma intromissão no domicílio e nas conversas deste, na medida em que permitirá ao investigador monitorizá-lo na sua habitação, sem o conhecimento dele, observando todos os seus movimentos e ouvindo todas as suas palavras.

Existe já, aliás, uma corrente doutrinária na Alemanha, que inscreve também na área da tutela da inviolabilidade do domicílio os casos em que a utilização de *malware* se traduz na monitorização do visado através da activação da câmara do seu computador, quando este se encontra na sua habitação.[80] Segundo esta corrente "também aqui se viola o domicílio, compreendido como o 'último refúgio' espacial para a expressão da intimidade e da privacidade (…). Também aqui se frustra a expectativa de entrincheiramento dentro das quatro paredes e se acede a dados que, de outra forma, só à custa da entrada arbitrária no domicílio seria possível alcançar."[81]

Sem prejuízo de reconhecermos que a utilização destes meios tecnológicos pode, efectivamente, traduzir-se numa violação da inviolabilidade do domicílio, seguimos, contudo, o entendimento sufragado pelo Tribunal Constitucional Federal Alemão no Acórdão BverfG,

---

[79] ANDRADE, Manuel da Costa, *"Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009, p.152

[80] Cfr. *Idem*, p. 153; esta foi, aliás, a posição adoptada pelo Governo Federal cfr. ABEL, Wiebke e SCHAFER, Burkhard, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BverfG, NJW 2008, 822", *SCRIPTed*, Volume 6, Issue 1, Abril 2009, pp. 111 e 115, disponível em http://script-ed.org/

[81] Na doutrina portuguesa, Benjamim Silva Rodrigues defende também a existência de um direito à inviolabilidade do domicílio informático cfr. Da Prova Penal – Tomo IV – *Da Prova Electrónico-Digital e da Criminalidade Informático-Digital,* Rei dos Livros, 2011 p.31. Na jurisprudência, veja-se, a título de exemplo o Acórdão do Tribunal da Relação de Guimarães, de 8 de Janeiro de 2014, proc. n.º 1170/09.8JAPRT.P2, onde se considera que o crime de acesso ilegítimo (artigo 6.º LC) tutela a integridade do sistema informático, a partir da ideia de "inviolabilidade do domicílio informático."

1 BvR 370, 595/07. Entende o Tribunal que este meio de obtenção de prova extravasa o objecto de tutela constitucional do direito fundamental à inviolabilidade do domicílio, na medida em que a intrusão em sistemas informáticos pode ter lugar independentemente da localização física do sistema alvo de investigação, pelo que um critério espacial não é suficiente, deixando de fora todos os casos em que o sistema informático visado se encontra fora do domicílio, não tomando assim em conta os riscos específicos dos sistemas de informação, tendencialmente caracterizados pela sua mobilidade.[82]

De facto, todas as situações em que o computador, *tablet* ou *smartphone* não se encontrem no domicílio, que podem ser tantas ou mais do que as situações em que aí se encontram, ficam fora do âmbito de tutela deste direito. Assim, conclui-se que uma protecção dependente da localização do aparelho informático é, no contexto actual, insuficiente.

6.4. O direito fundamental à confidencialidade e integridade de sistemas informáticos – a experiência Alemã

O Tribunal Constitucional Federal Alemão já teve oportunidade de se pronunciar especificamente sobre a problemática da infiltração em sistemas informáticos no Acórdão BverfG, 1 BvR 370, 595/07 que acima referimos, quando a Lei de Protecção da Constituição da Renânia do Norte-Vestefália foi alterada, tendo sido introduzida no seu §5.2.(11) uma norma que possibilitava a monotorização secreta e outras actividades de reconhecimento da *Internet*. O Tribunal parte da análise do problema à luz de três direitos fundamentais: o direito à privacidade da correspondência, o direito à inviolabilidade do domicílio e o direito à autodeterminação informacional.

Entendendo que nenhum destes direitos fundamentais conferia a tutela adequada à situação em apreço[83], sendo necessário um direito que tomasse "em suficiente consideração a

[82] Cfr. BverfG, 1 BvR 370, 595/07, de 27 de Fevereiro de 2008, versão inglesa disponível em http://www.bundesverfassungsgericht.de/en, especificamente sobre esta questão parágrafos 191 a 196

[83] Desenvolvimento detalhado do entendimento do Tribunal em ABEL, Wiebke e SCHAFER, Burkhard, "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 and Society*, Volume 6, n.º 1, Abril 2009, pp.112-122, disponível em http://script-ed.org/

necessidade de protecção que os desenvolvimentos tecnológicos reclamam,"[84] o Tribunal proclamou o direito fundamental à confidencialidade e integridade de sistemas informáticos, enquanto manifestação do direito geral de personalidade, decorrente da dignidade da pessoa humana. Entendeu o Tribunal que este direito será aplicável quando estejam em causa sistemas informáticos que possam conter dados pessoais de tal forma que o seu acesso permita o conhecimento de partes significativas da vida ou mesmo a construção de um perfil completo da personalidade do utilizador. É de louvar o Tribunal ter entendido que esta protecção se mantém independentemente desta capacidade de armazenamento de dados pessoais ser ou não utilizada no caso concreto – o que se protege é, efectivamente, o *sistema informático* em si mesmo e a susceptibilidade de este conter dados sensíveis, nomeadamente dados pessoais.[85]

De acordo com a formulação do Tribunal, este direito protege, em primeiro lugar, o interesse do utilizador em assegurar que os dados criados, processados e armazenados pelo sistema informático coberto pelo seu âmbito de protecção permaneçam confidenciais. Por outro lado, confere também protecção contra as intrusões ocultas, que permitam monitorizar os dados presentes no sistema, no seu todo ou em partes. Este direito protege também da aquisição de informação não dependente de sistemas de processamento de dados, como é o caso da utilização de *keyloggers*.[86] Salienta ainda o Tribunal que este direito existe, independentemente da maior ou menor dificuldade de acesso ao sistema de informação. Só existe, contudo, uma expectativa legítima de confidencialidade nos casos em que a pessoa visada utilize o sistema de informação como seu e possa, portanto, legitimamente presumir que só ela, e eventualmente outros da sua confiança, podem aceder aos dados nele contidos.[87]

O Tribunal Constitucional Federal veio, assim, a concluir pela inconstitucionalidade da norma, por violação do direito fundamental à integridade e confidencialidade dos sistemas

---

[84] NEVES, Castanheira, *As Ingerências nas Comunicações Electrónicas em Processo Penal,* Coimbra Editora, 2011, p. 200

[85] Cfr. BverfG, 1 BvR 370, 595/07, de 27 de Fevereiro de 2008, parágrafo 203 e ABEL, Wiebke e SCHAFER, Burkhard, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report n BVerfG, NJW, 2008, 822", *SCRIPTed – A Journal of Law, Technology and Society*, Volume 6, n.º 1, April 2008, p.120. disponível em http://script-ed.org/

[86] BverfG, 1 BvR 370, 595/07, de 27 de Fevereiro de 2008, parágrafo 204

[87] *Idem*, parágrafos 203 a 206

informáticos, concluindo ainda pela violação dos princípios da proporcionalidade, da clareza e da certeza legal. Contudo, é de salientar que não ficou excluída em absoluto a possibilidade de ser admitida a monotorização secreta e outras actividades de reconhecimento da *Internet* para fins de obtenção de prova, desde que respeitados os imperativos constitucionais que a Lei de Protecção da Constituição da Renânia do Norte-Vestefália violara.

Aliás, pouco depois, através da Lei para a Defesa Contra os Perigos do Terrorismo Internacional, de 25 de Dezembro,[88] veio a ser introduzida, na Lei da Polícia Criminal Federal,[89] a possibilidade de desenvolver investigações ocultas na *Internet*, sendo permitida a recolha de todos os dados que não digam respeito à esfera íntima do suspeito. É permitida a utilização de *keyloggers*, mas ficou excluída a possibilidade de activar remotamente a câmara ou o microfone do sistema informático visado.[90]

Apesar de ainda pouco desenvolvido na doutrina e na jurisprudência portuguesa, a integridade dos sistemas de informação tem sido invocada como sendo o bem jurídico tutelado pelo crime de falsidade informática (artigo 3.º LC), através do qual se "pretende impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados."[91] Não é, contudo, entendimento unânime. Veja-se, a título de exemplo, o Acórdão do Tribunal da Relação de Évora, de 19 de Maio de 2015, em que se considera que o crime de falsidade informática visa "proteger a segurança das relações jurídicas enquanto interesse publico essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos."[92]

---

[88] Disponível na íntegra em http://www.bgbl.de/

[89] No parágrafo 20k (*Verdeckter Eingriff in informationstechnische Systeme*) da Lei da Polícia Criminal Federal (*Bundeskriminalamtgesetz* - BKAG)

[90] Cfr. CUPA, Basil, "Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware)", *Living in Surveillance Societies: The State of Surveillance*, LISS, 2013, p. 422

[91] Acórdão do Tribunal da Relação de Lisboa de 30 de Junho de 2011, proc. n.º 189/09.3JASTBL.L1-5 e Acórdão do Tribunal da Relação do Porto de 24 de Abril de 2013, proc. n.º 585/11.6PAOVR.P1

[92] Acórdão do Tribunal da Relação de Évora, de 19 de Maio de 2015, proc. n.º 238/12.8PBPTG.E1

7. A utilização de *malware* e a possibilidade de restrição de direitos fundamentais

Importa não esquecer que os direitos fundamentais não são absolutos, podendo ter que ceder quando esteja em causa a necessidade de salvaguardar valores que realizam objectivos primários do Estado. Nos termos do artigo 18.º n.º 2 da CRP, contudo, "*a lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos*."

7.1.Previsão constitucional expressa

O primeiro pressuposto material da legitimidade das restrições ao exercício de direitos, liberdades e garantias consiste na exigência de previsão constitucional expressa da respectiva restrição, conforme resulta do artigo 18.º n.º 2 da CRP.

Nos termos do artigo 32.º n.º 8 da CRP, como já tivemos oportunidade de referir, são nulas todas as provas obtidas mediante *abusiva intromissão* na vida privada, no domicílio, na correspondência ou nas telecomunicações, de onde se retira, *a contrario,* que essas provas poderão ser obtidas e valoradas desde que a intromissão na vida privada não se tenha por abusiva. A intromissão será abusiva se, desde logo, não encontrar previsão legal expressa, como é aqui o caso. Ou seja, no quadro legislativo actual, a utilização de *malware* é inadmissível, por inexistência de previsão legal. Aquilo que pretendemos saber, contudo, é se existe a possibilidade de se vir a consagrar essa possibilidade na lei, pelo que importa analisar os restantes requisitos constitucionais.

7.2. Conflito de direitos ou de interesses constitucionalmente protegidos

O segundo pressuposto material para a restrição legítima de direitos fundamentais consiste na necessidade de existir um outro direito ou interesse igualmente merecedor de tutela constitucional.

No caso concreto, aquilo que se pretende salvaguardar é o princípio da investigação ou da verdade material e a realização da justiça. De acordo com o Tribunal Constitucional, "não

há dúvida de que o princípio da investigação ou da verdade material (…) tem valor constitucional. Quer os fins do direito penal, quer os do processo penal, que são instrumentais daquele, implicam que as sanções penais (…) apenas sejam aplicadas aos verdadeiros agentes do crime, pelo que a prossecução desses fins, isto é, a realização do direito penal e a própria existência do processo penal só são constitucionalmente legítimas se aquele princípio for respeitado."[93]

A verdade material não pode, contudo, ser obtida a todo o custo. Aliás, entende Germano Marques da Silva que não é correcto falar-se em verdade material, na medida em que "quando na dogmática processual se adjectiva a verdade que se busca no processo, pretende referir-se as limitações a que o tribunal está sujeito na sua busca e, por isso, se assume que a verdade processual não é necessariamente a verdade. A verdade processual não é senão o resultado probatório processualmente válido (…)."[94]

Assim, a busca da verdade e a realização da justiça têm limites impostos pela Constituição, nomeadamente o respeito pelos direitos fundamentais, decorrentes da dignidade da pessoa humana. Não é suficiente que a Constituição preveja a possibilidade de restrição e que existam dois ou mais direitos ou interesses constitucionalmente protegidos em conflito; é necessário, ainda, atender ao basilar princípio da proporcionalidade, segundo o qual a restrição se deve limitar ao estritamente necessário à protecção do interesse subjacente.

7.3. O princípio da proporcionalidade

Por último, como referimos, cumpre analisar a questão à luz do princípio da proporcionalidade, também chamado princípio da proibição do excesso. Este princípio é "a referência fundamental ao controlo da actuação dos poderes públicos em Estado de Direito, assumindo, particularmente no âmbito dos limites dos direitos fundamentais, o papel de principal instrumento de controlo da actuação restritiva da liberdade individual,"[95] podendo ser divido em três vertentes ou subprincípios: (a) o princípio da adequação ou da idoneidade, (b)

[93] Acórdão do TC n.º 137/02

[94] SILVA, Germano Marques da, *Curso de Processo Penal - II*, Editorial Verbo, 4.ª edição, 2008, p.130

[95] NOVAIS, Jorge Reis, *Os Princípios Estruturantes da República Portuguesa,* Coimbra Editora, 2004, p.161

o princípio da necessidade ou da exigibilidade e (c) o princípio da proporcionalidade em sentido estrito, que passaremos a desenvolver.

7.3.1. *O princípio da adequação ou da idoneidade*

O princípio da adequação ou da idoneidade significa que as medidas restritivas legalmente previstas devem ser adequadas a realizar os fins visados pela lei. Este controlo de adequação refere-se exclusivamente à "aptidão objectiva ou formal de um meio para realizar um fim e não a qualquer avaliação substancial da bondade intrínseca (…): uma medida é idónea quando é útil para a prossecução do fim." [96] Ou seja, neste primeiro momento de controlo é apenas necessário averiguar se a medida restritiva, no caso concreto a utilização de *malware*, é objectivamente adequada para a prossecução do fim visado, neste caso, a descoberta da verdade material e a realização da justiça.

Na amplitude de possibilidades que o *malware* coloca ao serviço da investigação criminal, dificilmente se pode concluir pela sua inadequação ou inidoneidade. Julgamos ser oportuno aqui referir alguns exemplos concretos da utilização de *malware* para fins de investigação criminal, permitindo uma melhor compreensão do seu funcionamento.

Em 1999, o FBI encontrava-se a investigar uma série de intromissões no sistema informático de uma empresa Americana, levadas a cabo com o objectivo de roubar informações financeiras das vítimas. Após identificação de um suspeito, Alexey Ivanov, os agentes do FBI instalaram fisicamente no seu computador *keyloggers*, através das quais obtiveram as credenciais de acesso ao servidor onde aquele guardava toda a informação relativamente aos crimes praticados, levando à sua acusação.[97]

Também em 1999, foram utilizados *keyloggers* pelo FBI, no âmbito de uma investigação criminal a Nicodemo S. Scarfo, suspeito de gestão de um negócio de jogo ilegal e de negócios usurários. No decurso de uma busca a sua casa, foi encontrado um computador,

[96] *Idem* p.167

[97] Maior desenvolvimento em JAHNKE, Art, "Alexey Ivanov and Vasiliy Gorshkov: Russian Hacker Roulette", *CSO*, 1 de Janeiro de 2005, disponível em http://bit.ly/1RwJsHc

ao qual o FBI tentou aceder. Contudo, alguns dos ficheiros encontravam-se cifrados, apenas podendo ser decifrados por quem tivesse a palavra-chave; suspeitando que esses poderiam ser importantes meios de prova para a acusação, foram instalados os *keyloggers*, que permitiram obter chave e decifrar os ficheiros em causa, que continham informação incriminatória.[98]

Em ambos os casos referidos supra, o *malware* foi instalado fisicamente nos computadores dos suspeitos. As dificuldades práticas que essa instalação suscita, bem como a evolução tecnológica, levaram ao desenvolvimento de programas que permitem a instalação remota de *malware,* nomeadamente do *Computer and Internet Protocol Adress Verifier* (CIPAV), utilizado pelo FBI. Este programa de *malware* permite recolher informações tais como o endereço de IP ou de MAC[99] do suspeito, a respectiva localização, a lista de programas em funcionamento, o sistema operativo utilizado (versão e número de série), a conta de utilizador aberta naquele momento e o último *website* visitado. Depois de recolhida esta informação, o CIPAV mantém-se oculto no sistema operativo do computador, monitorizando a utilização da *Internet* e registando os endereços IP das máquinas às quais aquele se ligou. É importante notar que este programa não permite aceder nem gravar o conteúdo das comunicações efectuadas através do sistema informático investigado. Só foi publicamente divulgado em 2007, apesar de haver relatos da sua utilização em anos anteriores.[100]

Em 2005, o FBI utilizou o CIPAV para obter a localização de um predador sexual que começara a ameaçar a vida de uma rapariga adolescente. A sua localização sem o recurso a este

[98] Maior desenvolvimento do caso em United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001), disponível em http://bit.ly/1T4Yc5z

[99] O endereço MAC (*Media Access Control*) é definido como sendo um endereço físico de uma placa de rede, e é composto por 12 caracteres. Os primeiros seis identificam o fabricante (ex. Intel) e os restantes seis identificam a placa em si. O endereço MAC é único no mundo para cada placa de rede. Mais informação em http://techterms.com/definition/macaddress

[100] Mais informação sobre o CIPAV em POULSEN, Kevin, "Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years", *Wired,* 16 de Abril de 2009, disponível em http://bit.ly/1MzfcKz e ORTIZ, Juan Carlos, "Remote Forensic Software as a Tool for Investigating Cases of Terrorism", *E-Newsletter on the Fight Against Cybercrime*, n.º 4, Outubro de 2009, pp.1-8, disponível em http://polis.osce.org/library/

malware não teria sido possível, pois este utilizava um *proxy*[101] para esconder o seu IP, impedindo o FBI de obter a sua localização ou outros dados que permitissem identificá-lo.[102]

Em 2007, o CIPAV foi utilizado para identificar o autor de várias ameaças de bomba dirigidas à Escola Secundária Timberline, em Washington. A primeira ameaça foi enviada por forma escrita, levando à evacuação da escola, mas nenhuma bomba foi encontrada. Dias depois, foi enviada uma segunda ameaça por e-mail, através de uma conta Gmail recentemente criada. O conteúdo do e-mail incluía "vou rebentar com a vossa escola na Segunda-Feira, dia 4 de Junho de 2007. Existem quatro bombas espalhadas pela escola." As ameaças foram repetidas várias vezes, sendo sempre enviadas de uma conta de Gmail diferente, sempre recentemente criada. O autor criou também uma conta *MySpace* para divulgar as suas intenções. Os agentes do FBI nunca conseguiam conseguir obter a sua localização até recorrerem ao CIPAV.[103]

Nestes termos, sem prejuízo de vários outros exemplos da utilização de *malware* para fins de investigação criminal, podemos concluir pela adequação objectiva da medida restritiva na procura da verdade material e na realização da justiça.

7.3.2. *O princípio da necessidade*

Num segundo momento importa verificar se a medida restritiva em análise se afigura como necessária, no sentido em que os fins visados pela lei não poderiam ser obtidos por outros meios menos onerosos para os direitos, liberdades e garantias. Ou seja, averiguar se não existe outro meio, que sendo igualmente idóneo para prossecução dos fins visados, seja sensivelmente

---

[101] Um *proxy* é um servidor (pode ser um computador ou outro dispositivo) que serve como intermediário para outros equipamentos. Equivale, por exemplo, a um servidor numa empresa que gere todo o tráfego da *Internet* que os seus colaboradores estão a fazer. Assim, em vez de cada colaborador aceder individual e directamente à *Internet*, na realidade efectuam pedidos ao servidor que, por sua vez, acede à *Internet* e devolve os resultados. Existem *proxys* anónimos, que incluem *software* que apaga o endereço de IP de todos os pedidos efectuados. Quando o servidor devolve os resultados apaga também quaisquer informações que possam comprometer a identidade do utilizador. Maior desenvolvimento em http://bit.ly/1XXFX1e

[102] Cfr. POULSEN, Kevin, "Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years", *Wired,* 16 de Abril de 2009, disponível em http://bit.ly/1MzfcKz

[103] Maior desenvolvimento em POULSEN, Kevin, "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats", *Wired*, 18 de Julho de 2007, disponível em http://bit.ly/1RwI3Xl

menos gravoso. Na ponderação das alternativas é, contudo, necessário que o nível de eficácia seja semelhante e que a eventual alternativa seja materialmente idêntica à medida original.

Assim, a medida restritiva será inconstitucional se for possível fazer prova da existência de um meio alternativo menos gravoso para os direitos fundamentais afectados ou, ainda, se a medida restritiva provocar efeitos mais gravosos do que as medidas actualmente em aplicação, sem garantir um acréscimo sensível de eficácia na realização do fim visado.[104]

Não logramos encontrar, em abstracto, um meio igualmente idóneo que se apresente, contudo, menos lesivo para os direitos fundamentais em apreço. Importa, ainda assim, verificar se os meios de obtenção de prova previstos na Lei do Cibercrime não se revelam já suficientes para a obtenção dos fins visados, de forma a averiguar da necessidade desta medida restritiva.

A Lei do Cibercrime prevê como meios de prova digital a preservação expedita de dados (artigo 12.º), a revelação expedita de dados de tráfego (artigo 13.º), a injunção para apresentação ou concessão do acesso a dados (artigo 14.º), a pesquisa de dados informáticos (artigo 15.º), a apreensão de dados informáticos (artigo 16.º), a apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º), a intercepção de comunicações (artigo 18.º) e as acções encobertas (artigo 19.º).[105]

Os artigos 12.º a 14.º destinam-se a regular as relações entre os fornecedores de serviços e as autoridades judiciárias, no que diz respeito à preservação, revelação e a obtenção de dados. Nos termos do artigo 12.º, sempre que, no decurso de uma investigação criminal, se afigure necessário, para a obtenção da prova, com vista à descoberta da verdade, a obtenção de dados informáticos específicos armazenados num sistema informático em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente – o juiz de instrução criminal, a pedido do MP (artigo 187.º n.º1 CPP)[106] – ordena

[104] NOVAIS, Jorge Reis, *Os Princípios Estruturantes da República Portuguesa,* Coimbra Editora, 2004, p.172

[105] A análise exaustiva destas medidas processuais é, no contexto do presente estudo, tarefa à qual não nos é possível dedicar. Para uma análise detalhada consultar VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada,* Coimbra Editora, 2010, p. 90 e seguintes

[106] RODRIGUES, Benjamin Silva, Da Prova Penal – Tomo IV – *Da Prova Electrónico-Digital e da Criminalidade Informático-Digital,* Rei dos Livros, 2011, p.521

a quem tenha disponibilidade ou controlo desses dados, designadamente um fornecedor de serviço (ou operadores de fornecimento de serviço de comunicações publicamente acessíveis) que preserve os dados em causa. Contudo, no actual contexto tecnológico, e tendo em conta os elevados conhecimentos informáticos e meios técnicos de que, em regra, estão dotados os cibercriminosos, é possível que os dados visados pela ordem da autoridade judiciária desapareçam antes que os fornecedores de serviços tenham possibilidade de os salvaguardar. Aliás, é mesmo possível configurar situações em que esses dados possam nunca chegar a vir a ser do conhecimento do MP, frustrando, assim, o objectivo da medida processual.

Os artigos 15.º e 16.º dizem respeito à pesquisa e apreensão de dados informáticos que forem encontrados e que se afigurem necessários à produção de prova, tendo em vista a descoberta da verdade. A sua leitura conjunta leva-nos à conclusão de que este regime não permite, desde logo, a obtenção de dados em tempo real[107], nem tão pouco parece permitir que essa pesquisa ou apreensão seja levada a cabo remotamente, i.e., sugere que tanto a pesquisa como a apreensão são efectuadas fisicamente no próprio sistema visado.

O artigo 17.º regula a apreensão de correio electrónico e registos de comunicações de natureza semelhante. Neste caso, estão em causa mensagens que, "após a sua recepção ficam armazenadas na caixa de correio do destinatário, seja em servidor que preste serviço de armazenamento (Webmail) ou no próprio computador do destinatário que as descarrega do servidor."[108] Acompanhamos Rita Castanheira Neves no entendimento de que o campo de aplicação da apreensão de correio electrónico se dirige a pesquisas informáticas já em curso, nos termos do artigo 15.º da LC, não se tratando da "possibilidade de obtenção de prova autónoma e independente,"[109] o que aliás parece resultar claramente da letra da lei. Assim, aquilo que dissemos a propósito daquele regime vale também aqui.

---

[107] Referimo-nos aqui, utilizando a terminologia da LC, a dados informáticos nos termos do artigo 2.º alínea b), e não a dados de tráfego e localização, i.e., "qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função"

[108] VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada,* Coimbra Editora, 2010, p. 120

[109] NEVES, Rita Castanheira, *As Ingerências nas Comunicações Electrónicas em Processo Penal*, Coimbra Editora, 2011, pp.273-274

O artigo 18.º regula a intercepção e registo em tempo real de comunicações, nomeadamente de correio electrónico e outros dados de tráfego,[110] dizendo respeito, portanto, exclusivamente às ingerências nas comunicações electrónicas. Como tivemos já oportunidade de referir, pensamos que aquilo se visa com a utilização de *malware* não é a intercepção de comunicações, mas sim atingir os ficheiros que integram o sistema informático. Conclui-se, assim, que a intercepção de comunicações regulada no artigo 18.º tem um objecto distinto daquele que se pretende atingir com a utilização de *malware*.

No que diz respeito ao artigo 19.º, relativamente às acções encobertas, como já analisamos, a sua formulação, nomeadamente do seu n.º 12, não permite a infiltração em sistemas informáticos através da instalação de *malware*; parece-nos que aquilo que resulta deste artigo é apenas a possibilidade de utilização de agentes encobertos, nos termos da Lei n.º 101/2001, de 25 de Agosto, em ambiente digital. Ou seja, permite levar a cabo "acções praticadas por agentes de investigação (da polícia ou sob o seu controlo), nas quais estes ocultam a sua qualidade e identidade (…) [de forma a] se introduzirem no meio dos suspeitos/arguidos (…) e de tentarem ganhar a confiança daqueles, de modo a (…) poderem acompanhar as actividades ilícitas, e assim conseguirem obter informações, recolher indícios ou elementos de prova das infracções investigadas."[111]

Não ignorando o esforço no sentido de adaptar as disposições processuais às realidades tecnológicas, nem a sua utilidade, e sem prejuízo do que já ficou dito a propósito de cada uma das medidas processuais, cumpre salientar alguma das hipóteses que a lei não prevê nem resolve. Em primeiro lugar, como já tivemos oportunidade de concluir previamente, nenhuma destas medidas possibilita a vigilância da actividade desenvolvida pelo utilizar no sistema informático ou a obtenção de dados, que não dados de tráfego, em tempo real, remotamente e sem o conhecimento do visado.

---

[110] Artigo 2.º alínea c) LC: «Dados de tráfego», os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

[111] COSTA, Eduardo Maia, "Acções Encobertas (Alguns Problemas, Algumas Sugestões)," *Estudos em Memória do Conselheiro Artur Maurício*, Coimbra Editora, 2014, p. 364

A lei também não parece ter em consideração, desde logo, as possibilidades de dissimulação de IPs, de ocultação de identidade, bem como de encriptação de dados que a tecnologia moderna possibilita, não prevendo, assim, mecanismos que permitam ao investigador criminal ultrapassar, de forma eficaz e em tempo útil, essas dificuldades.

Por outro lado, a lei também não permite nem prevê a possibilidade, por exemplo, de utilização de *keyloggers* com a finalidade de descoberta de palavras-passe. Este tipo de mecanismos revela-se de grande utilidade, permitindo ao investigador acesso a dados que estejam protegidos por palavra-passe, ao correio electrónico ou mesmo ao próprio computador.[112]

Podemos aqui concluir, em abstracto, que a Lei do Cibercrime é aparentemente insuficiente face aos desafios que as novas tecnologias colocam no prevenção e investigação criminal. Contudo, como deverá acontecer relativamente a qualquer método oculto de investigação criminal, a necessidade do meio terá que se aferir relativamente a um concreto catálogo de infracções criminais que o pretendem legitimar, nomeadamente um catálogo de crimes que se apresentem como suficientemente gravosos, pois como referimos a verdade material não pode ser obtida a qualquer custo.

Desde logo, o catálogo de crimes que eventualmente legitime o recurso à utilização de *malware* terá que ser mais reduzido do que o catálogo das acções encobertas ou das escutas telefónicas,[113] limitando-se aos casos mais graves em que os restantes meios de obtenção de prova se afigurem ineficazes ou, por outro lado, os casos em que a utilização de *malware* não se releve significativamente mais eficaz. Pensamos, nomeadamente, nos casos de organizações terroristas, terrorismo, terrorismo internacional e financiamento de terrorismo. Mas é também

[112] Também João Conde Correia refere a problemática das palavras-passe, focando-se na questão da inexistência de previsão legal da possibilidade da sua revelação coerciva – cfr. "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, Ano 35, n.º 139, Julho-Setembro 2014, pp.58-59

[113] Como salienta Costa Andrade a propósito das acções encobertas em "Métodos ocultos de investigação – *pläydoer* para uma teoria geral", *Que Futuro Para o Processo Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias por Ocasião dos 20 anos do Código de Processo Penal Português,* Coimbra Editora, 2009, p. 545

necessário que este catálogo respeite o princípio da proporcionalidade em sentido restrito, pelo que desenvolveremos esta questão infra.

7.3.3. *O princípio da proporcionalidade em sentido restrito*

Como referimos, não é suficiente concluir pela adequação e necessidade da medida restritiva, sendo necessário analisar a questão à luz do princípio da proporcionalidade em sentido restrito. Este princípio determina que os meios legais restritivos e os fins obtidos devem situar-se numa "justa medida"[114], impedindo a adopção de medidas desproporcionadas em relação aos fins obtidos. Ou seja, trata-se de, em concreto, "comparar sacrifícios (da liberdade individual) e benefícios obtidos ou visados, vantagens e desvantagens da restrição objecto do controlo."[115]

Assim, é necessário verificar se o sacrífico imposto ao direito à reserva da intimidade da vida privada não é desproporcionado em relação ao benefício que se espera obter com a utilização de *malware*. Deste modo, num primeiro momento, importa aferir das implicações da utilização de *malware* no direito fundamental à reserva da intimidade da vida privada.

Maior parte das pessoas utiliza diariamente sistemas informáticos para fins pessoais – seja um computador, um *tablet* ou um *smartphone* – onde guardam todo o tipo de dados e de informações. Actualmente, podemos dizer que estes dispositivos, bem como os arquivos neles armazenados, são como que uma "extensão da personalidade do seu proprietário".[116] A utilização de *malware* pode implicar que o investigador criminal obtenha informação pessoal armazenada naqueles sistemas, informação essa que se deva reconduzir àquela área inviolável da reserva da intimidade privada. Por exemplo, a pessoa alvo de investigação pode ter no seu computador ficheiros com conteúdos altamente pessoais, equiparáveis, por exemplo, a um diário íntimo, onde se possam encontrar registos atinentes à intimidade pessoal pertencentes ao

[114] CANOTILHO, Gomes J.J.; MOREIRA, Vital, *Constituição da República Portuguesa Anotada,* Volume I, Coimbra Editora, 2007, p.393

[115] NOVAIS, Jorge Reis, *Os Princípios Estruturantes da República Portuguesa,* Coimbra Editora, 2004, p. 179

[116] DRUMMOND, Victor, *Internet, Privacidade e Dados Pessoais,* Lumen Juris, 2003, p. 122

domínio absolutamente interno do seu autor.[117] O sistema informático investigado pode também conter imagens ou vídeos de conteúdo eminentemente pessoal.

Mais, ainda que o objectivo da utilização deste meio de obtenção de prova não seja a intercepção de comunicações, pode acontecer que, no decurso de uma vigilância da actividade desenvolvida pelo utilizador, sejam interceptadas mensagens, ainda que inintencionalmente, cujo conteúdo se deva também reconduzir àquela área inviolável da reserva da intimidade da vida privada. Apesar de não nos termos debruçado especificamente sobre a questão da inviolabilidade das telecomunicações, sempre se pode concluir que, em última instância, aquilo que visa tutelar é a privacidade dos cidadãos, na medida em que o que está em causa é "assegurar o *livre desenvolvimento da personalidade* de cada um através da troca, à distância, de informações, notícias, pensamentos e opiniões, à margem da devassa da publicidade."[118]

Aliás, a utilização de *malware* permite, genericamente, que o investigador observe, em tempo real, toda a actividade desenvolvida pelo utilizador: os ficheiros que abre, os documentos que lê, as páginas da *Internet* que consulta, os seus movimentos bancários, as pessoas com quem interage na rede, entre tantas outras possibilidades.

O acesso a todo este tipo de informações permite uma percepção clara das escolhas, dos gostos e do estilo de vida do utilizador, possibilitando que o investigador trace um perfil concreto da sua personalidade. De acordo com Paulo Pinto de Albuquerque, um dos limites materiais intrínsecos dos meios atípicos de prova é precisamente o da "inadmissibilidade da utilização, isolada ou coordenada, de meios de obtenção de prova que permitam uma 'vigilância total', uma vigilância 'global', com a qual possa ser construído um perfil completo da personalidade do arguido."[119]

Sempre se poderá argumentar que, ainda assim, existem outros meios ocultos de obtenção de prova que conferem a mesma possibilidade ao investigador – pense-se, por

[117] Sobre a questão da valoração de diários como meio de prova veja-se o Acórdão do TC n.º 607/03

[118] ANDRADE, Manuel Costa, "*Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009, p.158

[119] ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem,* Universidade Católica Editora, 2011, p.332

exemplo, no caso do agente encoberto, que se infiltre numa organização criminosa, com o objectivo de obter a confiança de determinado arguido ou suspeito, de forma a ter acesso a informações, planos, e confidências, com o fim de obter provas necessárias para a condenação daquele. Para obter esta confiança, o agente terá necessariamente que o conhecer também a um nível pessoal, podendo tomar conhecimentos da sua vida íntima, como seja da sua vida familiar, dos seus gostos pessoais, entre outros aspectos que em nada se relacionam com o objectivo da infiltração. Além disso, a acção poderá estender-se durante um período alargado de tempo, ao longo do qual se tornará seguramente possível que o agente construa um perfil da personalidade do arguido ou do suspeito em causa, ainda assim sendo um meio de obtenção de prova admissível no ordenamento jurídico português. Pense-se, ainda, no caso das escutas telefónicas, que permitem a intercepção e a gravação de conversações ou comunicações telefónicas (187.º n.º 1 CPP) pelo período de três meses, renovável por períodos sujeitos ao mesmo limite, sem o conhecimento dos visados. Também aqui facilmente se torna possível obter um perfil da personalidade do arguido ou do suspeito, pois serão também interceptadas conversas que se relacionam com a vida íntima daquele, e essa intromissão não deixa de ser verificar pelo facto de serem posteriormente destruídos os suportes técnicos que o juiz considere alheios ao processo, como sejam aqueles que possam colocar em risco direitos, liberdades e garantias [188.º n.º 6 alínea c) CPP].

Mais, a utilização de *malware* possibilita, como já tivemos oportunidade de ver, obter a localização geográfica do seu utilizador, permitindo ao investigador seguir, assim, não só os seus movimentos virtuais, mas também os seus movimentos físicos, obtendo, assim, informações de localização. Também, não é, contudo, o único meio de obtenção de prova que o permite – pense-se no caso da localização celular (252.º - A CPP).

O nível de sacrifício imposto é também influenciado pelo carácter oculto da medida. De facto, não tomando conhecimento da medida, o visado não pode fazer uso das suas garantias de defesa, como seja o direito ao silêncio. Ou seja, ao não ter conhecimento da medida secreta de investigação criminal, antes e durante a sua execução, "as pessoas atingidas não [podem] actualizar qualquer pretensão de reacção ou tutela dos seus direitos fundamentais."[120]

[120] ANDRADE, Manuel da Costa, "*Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009, p. 107

Refira-se ainda que, de acordo com os peritos ouvidos pelo Tribunal Constitucional Federal Alemão, não é possível excluir a possibilidade de a utilização de *malware* causar danos no sistema informático alvo da investigação. Por exemplo, as interacções com o sistema operativo podem levar à perda de dados, ficheiros, documentos, entre outros. É também de notar que com a utilização de *malware* não se pretende apenas a leitura de dados; a sua utilização permite, além de copiar, apagar, alterar ou criar novos dados, seja por acidente, seja por manipulação deliberada do sistema informático.[121]

Resulta claro que, não obstante a aparente adequação e necessidade da medida, estamos perante uma forte compressão dos direitos fundamentais, em especial no que diz respeito à reserva da intimidade da vida privada. Não é suficiente, como referimos a propósito da análise do subprincípio da necessidade, que exista, em abstracto, um catálogo de crimes que legitimem a medida. É necessário que o meio oculto de obtenção de prova seja "proporcional, enquanto meio particularmente invasivo, à gravidade concreta"[122] dos crimes em causa.

Assim, esta compressão tem que ser ponderada face aos casos em que seria de admitir a possibilidade de consagração de utilização de *malware*, nomeadamente em casos de organizações terroristas, terrorismo, terrorismo internacional e financiamento de terrorismo.

Julgamos que, nestes casos excepcionais, a restrição do direito fundamental à reserva da intimidade da vida privada respeita o princípio da proporcionalidade, não se afigurando excessiva, porquanto aqui a descoberta da verdade material apresenta como fim último acautelar valores constitucionais superiores, nomeadamente a vida e integridade física dos cidadãos, a realização do Estado de Direito e a realização da Justiça. Já nos parece excessiva a sua utilização para a investigação de crimes como o tráfico de estupefacientes, por exemplo, pois a relação entre o prejuízo para os direitos fundamentais dos suspeitos ou arguidos e o benefício que resultaria da restrição se apresenta como inadequada e, como tal, desproporcionada.

---

[121] Cfr. Acórdão BverfG, 1 BvR 370, 595/07, de 27 de Fevereiro de 2008, parágrafo 240

[122] COSTA, Eduardo Maia, "Acções Encobertas (Alguns problemas, algumas sugestões)", *Estudos em Memória do Conselheiro Artur Maurício,* Coimbra Editora, 2014, pp.361-362

Importa, contudo, não esquecer que, nos termos do artigo 18.º n.º 3 da CRP, as leis restritivas de direitos, liberdades e garantias não podem nunca diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais, ou seja, é necessário garantir que a restrição nunca leve, em última análise, à aniquilação do *núcleo essencial* dos direitos fundamentais atingidos. Seguimos aqui o entendimento de Gomes Canotilho e Vital Moreira, no sentido em que se deverá adoptar uma teoria mista na delimitação do núcleo essencial, i.e., tem de se articular com a necessidade de protecção de outros bens ou direitos constitucionalmente protegidos, mas, por outro lado, "é necessário que haja sempre um *resto substancial* de direito, liberdade e garantia, que assegure a sua *utilidade constitucional.*"[123]

[123] CANOTILHO, J.J. Gomes e MOREIRA, Vital, *Constituição da República Portuguesa Anotada,* Volume I, Coimbra Editora, 2007, p. 395

8. Conclusão

Ainda que concluindo pela possibilidade de, em casos verdadeiramente excepcionais, se admitir a consagração legal do recurso a *malware* para fins de investigação criminal, não podemos deixar de finalizar a presente dissertação com algumas advertências, tendo em conta a elevada eficácia intrusiva deste meio de obtenção de prova.

Em primeiro lugar, como já referimos previamente, a sua utilização tem obrigatoriamente que ser expressamente prevista por lei,[124] definindo-se claramente e de forma precisa os casos e em que termos essa utilização é possível, evitando deixar margens de interpretação que venham a permitir a sua utilização abusiva. É necessário que aí se estabeleçam limites à sua utilização, podendo o legislador colher as experiências de outros ordenamentos jurídicos, de forma a que a intromissão na privacidade dos visados seja o menos gravosa possível, proibindo-se a possibilidade de activar a câmara ou o microfone do sistema, bloqueando a possibilidade de interceptar as comunicações, bem como prevendo a eliminação imediata de toda a informação recolhida que se deva considerar integrante do núcleo inviolável da reserva da intimidade da vida privada, sem prejuízo de outras limitações que se devam estabelecer, pois só assim é possível manter intacto o *núcleo essencial* daquele direito fundamental.

É ainda imprescindível que se verifique, no caso concreto, "segundo os juízos de *plausibilidade e* probabilidade, (…) uma *suspeita fundada* da ocorrência de uma infracção do catálogo,"[125] suspeita essa que deverá ser "susceptível de comunicabilidade e escrutínio intersubjectivos."[126] Mais, é necessário que se faça sempre uma análise casuística do princípio da proporcionalidade, nas suas três vertentes, da utilização deste meio de obtenção de prova, tendo também sempre em mente o princípio da subsidiariedade, ponderando a possibilidade de

[124] Conforme o princípio da reserva de lei (18.º n.º 2 CRP), sendo que deverá ser uma Lei da Assembleia da República ou um Decreto-Lei do Governo devidamente autorizado, nos termos do 165.º n.º 1 alínea b) também da Constituição.

[125] RODRIGUES, Benjamim Silva, *As Novas Fronteiras do Direito no Dealbar do Século XXI*, Rei dos Livros, 2012, p. 28

[126] ANDRADE, Manuel da Costa, "Métodos ocultos de investigação – *pläydoer* para uma teoria geral", *Que Futuro Para o Processo Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias por Ocasião dos 20 anos do Código de Processo Penal Português,* Coimbra Editora, 2009, p. 546

existência de um outro meio oculto menos gravoso, ou mesmo de um meio "aberto" que se apresente como igualmente idóneo no caso concreto, recorrendo-se ao uso de *malware* apenas em casos extremos, de *ultima ratio*.[127]

Não esquecer também que, à luz do artigo 32.º n.º 4 da CRP, a autorização do uso deste método oculto terá que estar sujeita a "reserva de juiz (de Instrução)," com o objectivo principal de assegurar uma tutela preventiva de direitos fundamentais, já que o próprio visado não o pode fazer, por desconhecer da aplicação da medida. A autorização deverá ainda ser devidamente fundamentada, de forma, aliás, a possibilitar o seu escrutínio posteriormente, em sede de julgamento ou de recurso.[128] Assim, por último, exige-se que seja dado conhecimento aos suspeitos, arguidos ou visados após a realização da medida oculta, *in casu* da utilização de *malware,* "para que os mesmos controlem a legalidade da mesma e, acima de tudo, exerçam o contraditório."[129].

Se as tecnologias de informação trouxeram inegáveis benefícios para o desenvolvimento cultural, social e económico, a verdade é que vieram também permitir que a criminalidade no ambiente digital se desenvolvesse a um ritmo alarmante, ritmo esse que o Direito tem, por natureza, dificuldade em acompanhar. Estas novas modalidades de prática de infracções criminais colocam desafios ao Direito e, em especial, ao Direito Processual Penal às quais urge dar resposta. Assim, os meios ocultos de obtenção de prova aliados a este intenso progresso tecnológico apresentam possibilidades sem precedentes e de grande utilidade para a investigação criminal na resposta a estes desafios. Contribuem, contudo, para uma tensão cada vez maior e mais evidente entre a eficácia no combate ao crime e a protecção dos direitos fundamentais dos cidadãos, bem como para um esbater na fronteira entre prevenção e pressão criminal.

---

[127] Cfr. RODRIGUES, Benjamim Silva, *As Novas Fronteiras do Direito no Dealbar do Século XXI*, Rei dos Livros, 2012, pp. 30-31

[128] ANDRADE, Manuel da Costa, "Métodos ocultos de investigação – *pläydoer* para uma teoria geral", *Que Futuro Para o Processo Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias por Ocasião dos 20 anos do Código de Processo Penal Português,* Coimbra Editora, 2009p.548

[129] RODRIGUES, Benjamim Silva, *As Novas Fronteiras do Direito no Dealbar do Século XXI*, Rei dos Livros, 2012, p.35

A aplicação da inovação tecnológica na criação de novos meios de obtenção de prova é susceptível de trazer formas de ingerência nos direitos fundamentais cada vez mais graves. É imprescindível que se mantenha aqui um equilíbrio sustentável, combatendo a tendência para se afirmar um "Direito Penal do Risco". A evolução tecnológica, por muito útil que se possa revelar, não pode nunca determinar um retrocesso ao nível dos princípios estruturantes do Estado de Direito.

9. Bibliografia

ABEL, Wiebke e SCHAFER, Burkhard, "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 and Society*, Volume 6, n.º1, Abril 2009 - disponível em http://script-ed.org/

ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem,* Universidade Católica Editora, 2011

ANDRADE, Manuel da Costa, Anotação ao artigo 192.º do Código Penal, *Comentário Conimbricense do Código Penal – Parte Especial*, dirigido por Jorge de Figueiredo Dias, Coimbra Editora, 2012

- "*Bruscamente no verão passado", a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente,* Coimbra Editora, 2009
- "Métodos ocultos de investigação – *pläydoer* para uma teoria geral", *Que Futuro Para o Processo Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias por Ocasião dos 20 anos do Código de Processo Penal Português,* Coimbra Editora, 2009
- *Sobre as Proibições de Prova em Processo Penal,* Coimbra Editora, 1992

BOLDT, Martin, *Privacy-Invasive Software*, Blekinge Institute of Technology, 2010

CABRAL, Rita Amaral, "O direito à intimidade da vida privada (breve reflexão acerca do artigo 80.º do Código Civil)", *Estudos em Memória do Professor Doutor Paulo Cunha,* Faculdade de Direito de Lisboa, 1989

CANOTILHO, Gomes J.J.; MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volume I, Coimbra Editora, 2007

CLULEY, Graham, "*Facebook: There are over 83 million fake accounts on our site*", 2 de Agosto de 2015 – disponível em http://bit.ly/1pZoyKO

CONTE, Christiany Pegorari; FIORILLO, Celso Antonio Pacheco, *Crimes no Meio Digital*, Editora Saraiva, 2015

CUPA, Basil, "Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware)", Living in Surveillance Societies: The State of Surveillance, LISS, 2013

CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, Ano 35, n.º 139, Julho-Setembro 2014

COSTA, Eduardo Maia, "Acções Encobertas (Alguns Problemas, Algumas Sugestões)," *Estudos em Memória do Conselheiro Artur Maurício*, Coimbra Editora, 2014

DIAS, Jorge Figueiredo de, "Direito à informação, protecção da intimidade e autoridades administrativas independentes", *Estudos em Homenagem ao Professor Doutor Sérgio Soares*, Coimbra Editora, 2001

DIAS, Vera Marques, "A problemática da investigação do cibercrime", *Data Venia*, Ano 1, n.º 1, Julho-Dezembro, 2012 - disponível em http://www.datavenia.pt/

DRUMMOND, Victor, *Internet, Privacidade e Dados Pessoais*, Lumen Juris, 2003

ERBSCHLEO, Michael, *Trojans, Worms and Spyware – A Computer Security Professional's Guide to Malicious Code,* Elsevier Butterworth-Heinemann, 2005

FACHANA, João, "Reflexões sobre o anonimato no mundo digital", *Linhas Tortas*, Ordem dos Advogados – Conselho Distrital do Porto, Edição n.º 8, Maio de 2013, p.3 - disponível em http://bit.ly/1Rhr99C

FILIOL, Eric, *Computer viruses: from theory to application*, Springer, 2005

GALLAGHER, Sean, "Anonymous takes down darknet child porn site on Tor network", *Ars Technica*, 24 de Outubro de 2011 – disponível em http://bit.ly/1LDjyoZ

GOMES, Januário, "O problema da salvaguarda da privacidade antes e depois do computador", *Boletim do Ministério da Justiça*, n.º 319, Outubro 1982

INÁCIO, André, "Tecnologias de Informação e Segurança Pública: Um Equilíbrio Instável", *Revista Científica Sobre Cyberlaw*, CIJC, Faculdade de Direito de Lisboa, n.º 1, Janeiro 2016 – disponível em http://www.cijic.org/publicacao/

JAHNKE, Art, "Alexey Ivanov and Vasiliy Gorshkov: Russian Hacker Roulette", *CSO*, 1 de Janeiro de 2005 - disponível em http://bit.ly/1RwJsHc

JESUS, Francisco Marcolino, *Os Meios de Obtenção de Prova em Processo Penal*, Almedina, 2.ª edição, 2015

MENDES, Paulo de Sousa, *Lições de Direito Processual Penal*, Almedina, 2013

MOREIRA, João Manuel Dias, "O impacto do ciberespaço como nova dimensão nos conflitos", *Boletim Ensino|Investigação do IESM*, n.º 13, Novembro 2012

NEVES, Rita Castanheira, *As Ingerências nas Comunicações Electrónicas em Processo Penal,* Coimbra Editora, 2011

NOVAIS, Jorge Reis, *Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra Editora, 2004

PINHO, Carlos, "Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho", *Revista do Ministério Público*, Ano 33, n.º 129, Janeiro-Março 2012

PINTO, Paulo Mota, "O direito à reserva da intimidade da vida privada", *Boletim da Faculdade de Direito*, Volume LXIX, Coimbra, 1993

POULSEN, Kevin, "Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years", *Wired,* 16 de Abril de 2009 - disponível em http://bit.ly/1MzfcKz

– "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats", Wired, 18 de Julho de 2007 - disponível em http://bit.ly/1RwI3Xl

RAMALHO, David Silva, "A investigação criminal na *Dark Web*", *Revista de Concorrência e Regulação*, Ano IV, n.º 14/15, Abril-Setembro, 2013

– "O uso de *malware* como meio de obtenção de prova em processo penal" *Revista de Concorrência e Regulação*, Ano IV, N.º 16, Outubro-Dezembro 2013

RAMOS, Armando Dias, "A prova digital na investigação do (ciber)terrorismo", *Investigação Criminal*, n.º 9, ASFICPJ, Dezembro 2015

RODRIGUES, Benjamin Silva, *As Novas Fronteiras do Direito no Dealbar do Século XXI*, Rei dos Livros, 2012

– Da Prova Penal – Tomo IV – *Da Prova Electrónico-Digital e da Criminalidade Informático-Digital,* Rei dos Livros, 2011
– Da Prova Penal – Tomo II – *Bruscamente… A(s) face(s) oculta(s) dos métodos ocultos de investigação criminal*, Rei dos Livros, 1ª edição, 2010

SIEBER, Ulrich, *Legal Aspects of Computer Related Crime in the Information Society – COM-CRIME Study – prepared for the European Commission*, 1998

SILVA, Germano Marques da, *Curso de Processo Penal - II*, Editorial Verbo, 2008

SOARES, Maria, "Sweetie, a menina virtual que ajudou a encontrar predadores sexuais na *Internet*", *Público,* 5 de Novembro de 2013 - disponível em http://bit.ly/1ZnrjSa

ORTIZ, Juan Carlos, "Remote Forensic Software as a Tool for Investigating Cases of Terrorism", *E-Newsletter on the Fight Against Cybercrime,* n.º 4, Outubro de 2009 – disponível em http://polis.osce.org/library/

VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada,* Coimbra Editora, 2010