UNIVERSIDADE
LUSÓFONA

Centro Universitário de Lisboa

Faculdade de Direito

Mestrado em Direito

O *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA EM PROCESSO PENAL

Dissertação apresentada a provas públicas para a obtenção do grau de Mestre em Direito, orientada pelo Professor Doutor Bruno de Oliveira Moura

Teresa Alexandra Viegas Calvinho N.º 22109454

2024

UNIVERSIDADE
LUSÓFONA

Centro Universitário de Lisboa

Faculdade de Direito

Mestrado em Direito

O *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA EM PROCESSO PENAL

Dissertação de Mestrado defendida em provas públicas na Universidade Lusófona – Centro Universitário de Lisboa no dia 02/10/2024, perante o júri, nomeado pelo Despacho de Nomeação n.º Nº 892/2024, com a seguinte composição:
Presidente: Professor Doutor Joaquim Sabino Rogério
Arguente: Professor Doutor António Brito Neves (Faculdade de Direito da Universidade de Lisboa)
Orientador: Professor Doutor Bruno de Oliveira Moura

Teresa Alexandra Viegas Calvinho N.º 22109454

2024

Às minhas filhas, Tatiana e Miriam

Ao Sr. Dr. Antero da Silva Resende

Resumo

O termo *malware* resulta da contração do adjetivo *malicious* (malicioso) e do substantivo *software* (programa informático). À luz da informática, trata-se de um programa malicioso que é instalado ocultamente por outrem, num sistema informático, sem o conhecimento ou o consentimento do utilizador, sendo monitorizado em tempo real.

Com o intuito de combater uma criminalidade cada vez mais complexa, sobretudo os crimes perpetrados com recurso às novas tecnologias, os Estados adotaram novas medidas de carácter preventivo e repressivo, neste tipo delitos, pelo que gradualmente se percebeu a importância de ajustar os "cânones tradicionais" a este admirável mundo novo. As características da prova digital são muito peculiares, distintas das provas físicas, e sem qualquer paralelo de comparação, destacando-se a sua imaterialidade ou invisibilidade.

O recurso a um novo meio de obtenção de prova como *malware*, com vista à descoberta da verdade material, em circunstâncias que assim justifiquem, e em virtude dos obstáculos e dificuldades com que a investigação criminal se depara nos dias de hoje, face aos avanços da tecnologia, tornar-se-ia vantajoso, pois tal uso permitiria uma privilegiada obtenção de material probatório, determinante para a descoberta da verdade.

Colocou-se a como ponto de partida a seguinte questão: qual a utilidade do uso do *malware* como meio de obtenção de prova no processo penal?

Os resultados do estudo determinaram e sublinharam a natureza oculta e invasiva deste método de investigação, o que nos conduz para um conflito nas finalidades do processo penal, pois, por um lado, ostenta-se a sua admissibilidade para a descoberta da verdade, e para a realização da justiça, mas pode-se rejeitar a sua adoção, devido à elevada restrição dos direitos fundamentais em causa. Nesse sentido, vem-se a tender para que todas as soluções passem pela consagração legal do *malware*, da forma lúcida e harmoniosa.

Palavras-chave: admissibilidade; cibercrime; criminalidade; malware; meio de obtenção de prova; proibições de prova

Abstract

The term malware results from the contraction of the adjective malicious and the noun software (computer program). In the light of IT, this is a malicious program that is hiddenly installed (by some stranger,) on a computer system, without the user's knowledge or consent, and being monitored in real time.

In order to combat increasingly complex crime, especially crimes perpetrated using new technologies, States have adopted new preventive and repressive measures for this type of crime, which is why the importance of adjusting the "traditional canons" has gradually become clear to this "brave new world". The characteristics of digital evidence are very peculiar, distinct from physical evidence, with no direct comparison, highlighting its "immateriality or invisibility."

The use of a new means of obtaining evidence such as malware, with a view to discovering the material truth, in circumstances that justify it, and due to the obstacles and difficulties that criminal investigation faces today, in the face of advances in technology, would become advantageous, as the use of this means would allow obtaining evidentiary material that determines the discovery of the truth, especially when we are dealing with "more serious criminals".

The starting question was: what is the usefulness of using malware as a means of obtaining evidence in criminal proceedings?

The results of the study determined and highlighted the hidden and invasive nature of this method of investigation, which leads us to a conflict in the purposes of criminal proceedings, since, on the one hand, it is admissible for the discovery of the truth and the achievement of justice, but this adoption can be rejected due to the high restriction of the fundamental rights in question. In this sense, we are trying to ensure that all solutions involve the legal enshrinement of malware, in a lucid and harmonious way.

Keywords: admissibility; cybercrime; crime; malware; means of obtaining evidence; test bans

Lista de Abreviaturas

Ac. - Acórdão

AJ – Autoridade Judiciaria

CCiber - Convenção Cibercrime

CEDH - Convenção Europeia dos direitos humanos

CIPAV – *Computer and IP Address Verifier*

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

FBI – Federal Bureau of Investigation

FRCP - *Federal Rules of Criminal Procedure*

GG – *Grundgesetz* (Lei Fundamental/Constituição da República da Alemanha)

GSM – *Global System for Mobile Communications*

IP – Internet Protocol

JI - Juiz de Instrução

LC – Lei do Cibercrime

MAC - *Media Access Control*

OPC – Órgãos de Polícia Criminal

Op. cit. – Da obra citada

P., PP. – página, páginas

MP – Ministério Publico

RJAE – Regime Jurídico das Ações Encobertas

StGB – *Strafgesetzbuch* (Código Penal Alemão)

STJ – Supremo Tribunal de Justiça

StPO – *Strafprozeßordnung* (Código de Processo Penal Alemão)

TC - Tribunal Constitucional

TEDH – Tribunal Europeu dos Direitos do Homem

TOR – *The Onion Router*

TRL – Tribunal da Relação de Lisboa

UFED - Universal Forensic Extraction Device

“Onde não há lei, não há liberdade”.

John Locke

Índice

Introdução

A questão central para a presente dissertação reside no atual estágio de avanço e penetração social das novas tecnologias de informação e comunicação, na procura de uma redução de custos, e da agilidade de comunicação nas redes, entre outras finalidades, que na prática se traduzem numa crescente facilidade de modalidades criminosas.

São reflexos que se sentem nos comportamentos individuais e nos diversos setores da vida social, como a educação, o trabalho, o lazer e as compras, tendo estes efeitos diretos no Direito[1]. É com base neste pressuposto que se observa o surgimento do cibercrime[2] e a urgência do Estado na obtenção das provas em formato digital, especialmente para a instrução de processos de natureza criminal.

Desta forma, começou a ser utilizado um novo e controverso meio de obtenção de prova, em matéria criminal, o *malware*, que, muito sumariamente, se trata de um tipo de *software* que é instalado de forma oculta no equipamento ou sistema informático do visado, a partir do qual será possível a recolha de prova interna e/ou externa, quando o sistema informático comporte a ativação do *hardware*

Segundo Manuel da Costa Andrade[3], as ferramentas de *malware* constituem formas de intromissão e abuso dos sistemas informáticos, reconduzíveis ao conceito de busca *online*. Tal conceito, abrangente, mas, porventura, não inteiramente rigoroso, acolhe, na visão deste Autor, todo um conjunto de intromissões nos ditos sistemas, através da *internet*. Esse conjunto inclui observação, busca, cópia e vigilância dos dados presentes nos mesmos sistemas informáticos.

A necessidade e a utilidade de recurso aos métodos ocultos para a obtenção de prova, conduziu à reflexão sobre os conflitos emergentes das finalidades do processo

[1] PRADILLO, Juan Carlos Ortiz. «Remote Forensic Software as a tool for Investigating Cases of Terrorism». ENAC. Outubro de 2009. p. 1.
[2] Num conceito amplo abarca toda criminalidade informática, cibercriminalidade o cibercrime como um facto típico tipificado na lei como crime que é praticado através da utilização de um sistema informático na aceção do artigo 2.º, al, a) da lei 109 /2009. NUNES, Duarte Alberto Rodrigues. *Os meios de obtenção de prova previstos na Lei do Cibercrime*. 2ª Edição revista e atualizada, Gestlegal, 2021. pp. 37- 45
[3] 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: Editores Coimbra, 2009. p. 166.

penal nesta área, na descoberta da verdade material e a efetivação da justiça, sopesadas com a proteção dos direitos fundamentais dos cidadãos.

Como ponto de partida coloca-se a questão: pode o Estado, à semelhança de um *hacker*[4], aceder remotamente, através de *malware*, a informações existentes no nosso computador? sem o nosso conhecimento, desde que no âmbito de uma investigação criminal?

Tendo em conta os pressupostos apresentados, a análise terá como base a reflexão sobre a utilização do *malware* como meio de obtenção de prova no processo penal, exigindo, assim, uma contextualização do tema e uma explanação da sua utilidade e relevância prática, no âmbito da investigação criminal, assim como uma identificação do impacto sobre os direitos fundamentais e garantias processuais do sujeito investigado.

Após a delimitação conceptual, apresentaremos a discussão atual quanto a este meio de obtenção de prova. Em seguida, analisaremos alguns preceitos do CPP, a fim de demonstrar que o *malware* é um meio de obtenção de prova distinto, e que comporta uma potencial violação dos direitos fundamentais, pelo que não pode ser indiscriminadamente legitimado qualquer preceito, sob pena de inconstitucionalidade material.

Procederemos a uma análise dos meios de obtenção de prova interna de dados armazenados nas pesquisas dos dados informáticos (artigo 15.º da LC), da apreensão de dados informáticos e da apreensão de correio eletrónico (artigos 16.º e 17.º da LC), de dados produzidos em tempo real (artigos 18.º e 19.º da LC) e, ainda, dos meios de obtenção de prova externa, ou seja, das intersecções das comunicações entre presentes (n.º 1 do artigo 189.º do CPP) e do registo de voz e imagem, artigo 6.º das medidas de combate à criminalidade organizada Lei n.º 5/2002, de 11 de janeiro. Será ainda feita uma breve passagem pelos métodos atípicos de prova, e pelo impossível enquadramento do *malware* nos meios atípicos de prova, nos termos do artigo 125º do CPP.

[4] *Hacker*, alguém que acede ou decifra. Em informática, é o nome dado a determinada pessoa que se dedica, quer profissionalmente quer de forma amadora ainda que com grande intensidade, a explorar ou alterar equipamentos ou programas informáticos, em redes de computadores. A sua ação poderá ser exercida por acessos a informações privilegiadas, por desafios, lazer, ou para avaliação ou deteção de pontos fracos de sistemas informáticos promovendo uma constante reformulação de proteções. SCHWALBACH, José Gaspar. *Direito Digital*, 2.º Edição, Almedina, 2021. p. 44.

Debruçar-nos-emos também sobre a previsão do *malware* nos ordenamentos jurídicos espanhol, americano e alemão tendo em conta que estes ordenamentos foram alvo de recentes alterações tendo a consagração do tema sido expressa. Apresentaremos ainda uma breve síntese da experiência portuguesa.

Por fim, serão indicados os requisitos formais, materiais e orgânicos, que consideramos indispensáveis, para que uma lei que proceda à consagração da matéria no nosso ordenamento jurídico seja constitucional e legalmente admissível.

CAPÍTULO I: A UTILIZAÇAO DO *MALWARE* EM SISTEMAS INFORMÁTICOS NO ÂMBITO DA INVESTIGAÇÃO CRIMINAL

1. Discussão atual

Assiste-se hodiernamente a uma evolução sem paralelo das tecnologias da informação e da comunicação. Em simultâneo, vislumbra-se uma crescente relação entre o ser humano e os sistemas informáticos, potenciando-se a interação entre as pessoas, amiúde sem que as mesmas se conheçam, o que altera por completo o paradigma das relações humanas.

De fácil acesso, a *internet*[5] entrou nas nossas casas, nas nossas vidas, simplificando a aquisição de bens e serviços, o acesso à informação e à comunicação, a possibilidade de transações bancárias, e um sem fim de opções, sem que nos tenhamos de deslocar.

Todavia, esta evolução tecnológica não apresenta apenas vantagens, pois, se por um lado facilitou a vida dos utilizadores, por outro veio abrir novas vias para o cometimento de ilícitos, facilitando a anonimização, tanto de identidade como de localização dos agentes do crime.

Como é sabido, "o crime tende a seguir a oportunidade"[6] e a *internet* é fértil em propiciar oportunidades. Assim, tem-se vindo a observar uma deslocação "da criminalidade, do mundo físico para o mundo virtual"[7], pois se tornou cómodo para os criminosos convencionais praticar os mesmos crimes com muito menos riscos.

[5] *Internet* , significa entre redes, nome pelo qual é atualmente conhecida aquela que se pode designar por redes de computadores interligadas, que utilizam um conjunto próprio de protocolos (Internet Protocol Suite ou TCP/IP) com a finalidade de servir os usuários no mundo inteiro à qual pode aceder qualquer tipo de utilizador, e que possibilita o acesso. Disponível em https://www.infopedia.pt/artigos/$internet (consultado em 02/04/2024).

[6] PELLUCI, Frederico. A atuação dos agentes encobertos e infiltrados nos canais abertos e fechados de comunicação em ambiente informático-digital. In: *Novos desafios da prova penal* / coord. Paulo de Sousa MENDES, Rui Soares Pereira. Coimbra: Almedina, 2020. p. 237.

[7] *Idem*, p. 239.

É neste horizonte que o fenómeno da cibercriminalidade se torna transnacional, alastrando-se de forma descontrolada, desconhecendo muros, fronteiras ou continentes e, sem que nos apercebamos da sua presença, instala-se no nosso quotidiano. Se "houve um tempo em que a polícia não precisava de mais do que uma arma, um par de algemas, um bloco de notas e os próprios sentidos, para desempenhar as suas funções"[8], nos dias de hoje, a nova era da "ciber-sociedade" exige que a investigação criminal, para além dos tradicionais métodos, (apreensões, buscas domiciliárias, escutas telefónicas, entre outros), recorra a novos métodos de investigação e novos meios de obtenção de prova, pelo que se impõe ao legislador um constante esforço, na criação de meios excecionais de combate a esse tipo de crime.

Porém, esta nova realidade, mais sofisticada de meios materiais e humanos, veio acarretar problemas específicos, em matéria de processo penal, colocando novos desafios à justiça e aos seus operadores judiciários[9], o que levou o legislador penal a consagrar um novo regime jurídico, com a aprovação da Lei 109/2009, de 15 de setembro, a chamada Lei do Cibercrime.[10]

Contudo, se o desenvolvimento das tecnologias veio facilitar a vida em geral, assim também ficou o investigador, órgãos de investigação criminal, dotado de equiparada vantagem tecnológica. A Lei do Cibercrime veio introduzir novas medidas processuais, em matéria de produção de prova. Neste contexto, em vários países, as AJ e os OPC passaram a adotar novos meios de obtenção de prova de natureza oculta. Falamos do uso de *malware,* como meio de obtenção de prova.

A utilização do *malware* na investigação criminal decorre do impacto significativo protagonizado pela informática no âmbito jurídico. É neste contexto que, em vários países, as AJ passaram a adotar novos meios de obtenção de prova, de natureza oculta, no âmbito da investigação criminal, como meios de obtenção de prova.

---

[8] PRADILLO, Juan Carlos Ortiz. "La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación." *Revista Estudios de Progresso*. 2013. p. 8.

[9] VALENTE, Manuel Monteiro Guedes, *Teoria geral do direito policial*, 6ª edição, Almedina, 2019, p. 627.

[10] Resultante da Convenção sobre o Cibercrime, 23 novembro 2001, e transposta para o nosso ordenamento jurídico, mediante Decisão-Quadro n.º 2005/222/JAI, do Conselho, relativa a ataques contra sistemas de informação, assim dando origem à Lei n.º 109/2009, de 15 de setembro, que revogou a Lei da Criminalidade Informática – Lei n.º 109/91, de 17 de agosto.

Desta forma, dada a abrangência demonstrada pelo *malware*, como meio de recolha de prova, vários ordenamentos jurídicos, como americano, o alemão e o espanhol, introduziram alterações legislativas, com a finalidade de integrar e legitimar o recurso a este meio.

Como já dito, o *malware* é um software malicioso instalado clandestinamente pelas Autoridades no sistema informático do suspeito, posto avançado destinado à quebra da confidencialidade e integralidade dos dados nele contido[11].

Uma vez instalado, possibilita a extração e/ou a destruição de dados, permite acesso a informações, documentos ou, ainda, a monitorização do suspeito em tempo real, sem o conhecimento.

Trata-se, como se constata, de um meio oculto de obtenção de prova que conflitua com as finalidades do direito processual penal, na descoberta da verdade, e com os limites que salvaguardam os direitos fundamentais. Assim, a permissão da utilização deste meio significa consentir a investigação e obtenção de elementos probatórios, com vista à descoberta da verdade, mas, tal como com outro método oculto, há que considerar a restrição a direitos fundamentais, não só na esfera jurídica do visado, mas também na de um outro dado número de pessoas.[12]

Em suma, esta nova realidade obrigou o nosso legislador à criação de diplomas especiais, os quais foram criados autonomamente à medida das necessidades da investigação criminal. No entanto, quando concatenados com o CPP e a CRP, acabam por permanecer afastados, quando não em conflito.

2. Enquadramento do direito do cibercrime

A grande evolução, nas últimas décadas, das tecnologias da informação e comunicação, em particular o desenvolvimento da *internet*, favoreceu o processo de globalização económica e cultural e, consequentemente, o progresso. Tendo emergido,

[11] JR, Aury Lopes; MENDES, Carlos Hélder Carvalho Furtado. Vírus espião" como meio de investigação: a infiltração por softwares. *Revista Consultor Jurídico*. Disponível em https://www.conjur.com.br/2019-jun-07/limite-penal-virus-espiao-meio-investigacao-infiltracao-softwares/ (consultado em 16/03/2024).
[12] CAMPOS, Juliana Filipa Sousa, *O malware como meio de obtenção de prova em processo penal*. Coimbra Almedina, 2021. p. 55.

consequentemente, novas formas para o cometimento de ilícitos, foi-se levado à construção de novos diplomas legais, na área do cibercrime[13], pelo que consideramos relevante uma curta apresentação sobre a evolução legislativa.

No início da passada década de 90, do século XX, Portugal aprovou pela primeira vez uma lei integralmente dedicada à cibercriminalidade, a Lei n.º 109/91, de 17 de agosto, Lei da Criminalidade Informática, que era um diploma simples, de conteúdo essencialmente substantivo, adotando as medidas que viriam a constar da Convenção de Budapeste, e que vinham já sendo debatidas e harmonizadas na comunidade internacional havia vários anos[14].

O grande contributo da Lei da Criminalidade Informática no nosso ordenamento foi a introdução dos principais tipos legais dos crimes, em sentido estrito, ainda não previstos no código penal de 1982, como a falsidade informática, o dano relativo a dados ou programas informáticos, a sabotagem informática, o acesso ilegítimo, a interceção ilegítima e a reprodução ilegítima de programa protegido[15].

Não obstante, a Lei 109/91, de 17 de agosto era um diploma adequado a época, destinando-se a regular a matéria, tendo-o feito no decurso de quase duas décadas, mas que se tornou-se deficitário. De facto, surgiram novas "redes de informação e comunicação, surgiram entretanto novas realidades que têm vindo a ser descritas e consideradas como crime por muitas outras legislações europeias e por instrumentos internacionais"[16]. Tal é o caso da produção e difusão de vírus e outros programas maliciosos, realidade então não consagradas na lei nacional.

---

[13] Na doutrina, são apresentados vários conceitos de cibercrime, distinguindo os autores entre a criminalidade informática em sentido amplo e em sentido estrito. Em sentido amplo, a criminalidade informática englobará toda a panóplia de atividades criminosas que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais do que instrumentos, e as mesmas atividades possam ser cometidas por outros meios. Em sentido estrito, a criminalidade informática abarcará aqueles crimes em que o elemento digital surge como integrante do tipo legal ao mesmo com o seu objeto de proteção. O conceito amplo abarca toda criminalidade informática, cibercriminalidade o cibercrime como um facto típico tipificado na lei como crime que é praticado através da utilização de um sistema informático na aceção do artigo 2.º, al, a) da lei 109 /2009. NUNES, Duarte Alberto Rodrigues. *Os meios de obtenção de prova previstos na Lei do Cibercrime*. 2ª Edição revista e atualizada, Gestlegal, 2021. pp. 37-45

[14] VENÂNCIO, Pedro Dias, *Lições de Direito do Cibercrime e* da tutela penal de dados pessoais. Coimbra, Editora D'Ideias. 2022. p. 58-59

[15] *Idem*, p. 60

[16] Exposição de motivos da proposta de Lei nº 289/X/4ª, Lei do Cibercrime, p. 1.

Assim, com a Resolução da Assembleia da República n.º 88/2009[17] e o Decreto do Presidente da República n.º 92/2009, ambos publicados a 15 de setembro, Portugal ratificou a Convenção sobre cibercrime, adotada em Budapeste em 20/03/2001 e, na mesma data, foi publicada a lei 109/2009[18], de 15 de setembro, denominada Lei do Cibercrime, que revogou a Lei da Criminalidade Informática, assim se transportando para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho da Europa, de 24 fevereiro.

Com a entrada em vigor desta lei, foram estabelecidas as disposições penais materiais e processuais, também as disposições relativas à cooperação Internacional em matéria penal, no domínio do cibercrime e da recolha de prova em suporte eletrónico, tendo-se em consideração o tipo de criminalidade estar associado a práticas além-fronteiras, o que criava obstáculos à aquisição de prova e à celeridade necessária à cessação das atividades criminosas[19].

O catálogo de crimes tipificados na Lei 109/2009 de 15 de setembro manteve-se idêntico ao da Lei de 1991, mas ela passa a conter um conjunto de disposições processuais aplicáveis a crimes que constem da LC, cometidos por meio de sistema informático e a qualquer outro em relação ao qual seja necessário proceder a prova em suporte eletrónico, ou seja, disposições processuais relacionadas com a prova digital.

Esta alteração teve como finalidade superar o atual regime, fornecendo ao sistema processual penal normas que permitam a obtenção de dados de tráfego e a realização de interceções de comunicações em investigações de crimes praticados no ambiente virtual[20].

No âmbito das disposições processuais, foram introduzidas a preservação expedita de dados armazenados num computador e a preservação expedita e revelação de dados de tráfego, em cumprimento das obrigações resultantes dos artigos 16º e 17º da Convenção.

Foi introduzido o mecanismo da injunção (cfr. artigo 18º da Convenção) e adaptados os regimes das buscas e das apreensões, já largamente previstas na legislação processual penal, às investigações de crimes cometidos no ambiente virtual. Na verdade,

[17] https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1505&tabela=leis (consultado em 18/03/2024)
[18] Alterada pela lei n.º 79/2021, 24 de novembro.
[19] SCHWALBACH, José Gaspar. *Direito Digital*, 2.º Edição, Almedina, 2021. p. 23.
[20] Exposição de motivos da proposta de Lei nº 289/X/4ª, Lei do Cibercrime, p. 3.

a essência destas medidas processuais coincide, no ambiente do ciberespaço, com as clássicas formas de busca e apreensão do processo penal. Porém, a forma como a busca e a apreensão estão descritas no Código de Processo Penal exigiam alguma adequação a estas novas realidades.[21]

Contudo, embora a proposta de Lei n.º 289/4ª, de 21 de maio de 2009, tivesse como finalidade atualizar e aperfeiçoar a legislação de combate ao cibercrime, em linha com os padrões do Conselho da Europa e da União Europeia, o diploma não contemplou a possibilidade de as entidades de investigação criminal introduzirem o "«cavalo de Tróia informático», para poder obter informação contínua e em tempo real, assim facilitando as investigações criminais, designadamente através dos meios informáticos"[22].

Conquanto a Lei do Cibercrime fosse um diploma inovador, na verdade, a interpretação e a sua aplicação, conjuntamente com as normas aplicáveis neste domínio, bem como a prova digital, têm suscitado algumas dúvidas na doutrina e na jurisprudência nacionais, nomeadamente quando são invocados vários institutos de diplomas diferentes, ou a articulação entre a Lei do Cibercrime e o Código de Processo Penal, em conformidade com o regime jurídico relacionado com a conservação dos dados gerados e tratados no contexto das comunicações eletrónicas (Lei n.º 32/2008, de 17 de julho) e com o Direito da União Europeia.

Mais recentemente, a 8 de maio de 2021, o Presidente da República promulgou a Carta Portuguesa dos Direitos Humanos na Era Digital , que viria a ser publicada a 17 do mesmo mês, Lei 27/2021, que veio consagrar no ordenamento jurídico português, pela primeira vez, direitos em ambiente digital e acesso ao ambiente digital avançado, quanto à liberdade de exposição e criação em ambiente digital e à garantia de acesso e uso das redes de informação, impedindo que possa ser colocado em causa o acesso à *Internet*, ao mesmo tempo que se estabelece o novo direito à proteção contra a desinformação.

[21] *Idem*, pp 4-5.
[22] Diário da Assembleia da República, I Série, n.º 102/X/4, de 09-07-2009. pp. 40-44, disponível em http://debates.parlamento.pt/catalogo/r3/dar/01/10/04/102/2009-07-10/40?pgs=40-45&org=PLC (consultado em 21/03/2024).

3. O *Malware*: Noção, modalidades e funcionalidades

O termo *malware* resulta da contração do adjetivo *malicious* (malicioso) e do substantivo *software* (programa informático)[23]. À luz da informática, trata-se de um programa malicioso que é instalado ocultamente por terceiros, num sistema informático, sem o conhecimento, do utilizador, sendo monitorizado em tempo real.

Nas palavras de David Silva Ramalho, o *malware* pode ser definido como "programa simples ou autorreplicativo que discretamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a comprometer a confidencialidade dos dados, a integridade dos dados e a disponibilidade do sistema, ou para assegurar que o utilizador seja incriminado por um crime informático"[24].

Com efeito, o conceito *malware* comporta uma certa amplitude, isto é, abrange todo o tipo de programas instalados, por um terceiro não usuário, sub-repticiamente, num sistema informático e que, eventualmente, pode ser utilizado para comprometer as suas funções, contornar os seus controlos de acesso, causar prejuízo ao utilizador ou ao sistema informático infetado, ou monitorizar a atividade em tempo real, tal como hábitos do utilizador, horas de acesso, páginas visitadas ou, ainda, apropriar-se de dados armazenados, ou eliminando ou alterando os mesmos.

No que concerne à utilização do *malware* em contexto de investigação criminal, em regra, a doutrina refere-se somente aos "cavalos de Tróia". Contudo, os "cavalos de Troia" representam um de muitos tipos de *malware*, aptos para uso nas investigações criminais em ambiente digital, a par de outros softwares (*logic bombs*, os *rootkits*, o *spyware* e *worms*), que abrangem mais de uma modalidade de *malware*.[25]

É, portanto, consabido que existem vários tipos de *malware*. Porém, não podemos abordar todos eles, pelo que apenas trataremos os mais relevantes para a investigação criminal. O *malware* pode ser classificado atendendo a vários aspetos: Um primeiro, quanto à forma com que se propaga e um segundo, quanto à sua funcionalidade. Assim,

---

[23] RAMALHO, David Silva, *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra: Almedina, 2017. p. 318-319.
[24] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 319.
[25] *Idem*.

quanto à forma como o *malware* se propaga, comecemos por referir que estes programas se podem dividir em dois grupos: os que necessitam de um comportamento voluntário ainda que enganado) do utilizador para a propagação (como é o caso do cavalo de Troia, dos *rootkits* e do *spyware*) e os que não carecem da intervenção do utilizador (*worms*).

O segundo aspeto refere-se às diversas funcionalidades deste tipo de programas, que divergem todas entre si. Iniciando pela conceção mais utilizada, a dos cavalos de Troia, ela pode ser definida como um tipo de *malware* que se assemelha a um *software* legítimo, aparentemente inofensivo, e que induz ao utilizador a instalação do programa voluntariamente (por exemplo, fazer o *download* de um anexo ao *e-mail*, ou abrir uma página *web* infetada com um outro código malicioso)[26].

Uma vez instalado, tem diferentes tarefas no equipamento, desde recolher ou destruir dados, monitorizar o utilizador, entre outros, sem que o utilizador se aperceba[27]. Outras vezes, os cavalos de Tróia podem ser utilizados para criar *backdoors* no sistema informático infetado, permitindo aceder remotamente ao sistema de forma oculta, ao tornear os mecanismos de autorização presentes no sistema.

Por seu turno, as *logic bombs*[28] são outra modalidade de *malware*, não replicativo, que se instala no sistema informático e "aguarda um incidente", uma ação que opere como elemento desencadeador para realizar uma "função nociva ou ofensiva" no sistema informático infetado, ou seja, funcionando como um gatilho que é ativado de acordo com a finalidade do *hacker*.

No que diz respeito aos *rootkits*, a instalação ocorre nos mesmos moldes que a do cavalo de Tróia, o que permite ao intruso aceder privilegiadamente, como administrador, a um sistema informático, através da exploração de uma vulnerabilidade do sistema operativo, a descoberta de uma palavra-passe. Em regra, os *rootkits* são utilizados para

[26] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 320.
[27] CAMPOS, Juliana Filipa Sousa, *O malware como meio de obtenção de prova em processo penal*. Coimbra Almedina, 2021. p. 38.
[28] *Logic bombs*, exemplo avançado por Eric Filiol, "o caso do administrador de rede que instala no sistema informático da empresa onde trabalha uma *logic bomb* programada" para obter informação diária, se o seu nome ainda se encontra no registo da contabilidade. Assim, quando administrador deixar de trabalhar na referida empresa, a "*logic bomb* ativa-se e cifra todos os documentos da empresa, incluindo os *backups,* com uma chave secreta, e tornam-se potencialmente indecifráveis". RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. pp. 320-321.

esconder outro tipo de *malware*, como o cavalo de Tróia ou o *spyware*, sendo assim estes impercetíveis perante o *antivírus* ou *anti-spyware* vigentes.

O *spyware* é um *software* normalmente utilizado como *keylogger* (software/*malware* dependendo da finalidade), definido como programa informático que recolhe informações sobre uma pessoa, efetua a monitorização do utilizador, ou vigia a atividade do utilizador sem o seu conhecimento. Pode ser instalado no sistema informático através de um "cavalo de Tróia", como um vírus, ou ao se aceder a um *website* malicioso.[29]

Por último, o *worm*, outro tipo de *software* que se replica autonomamente na rede, não necessitando da intervenção humana, e cuja propagação se dá por meio de falhas de segurança presentes no *software* do sistema informático do visado, ao qual pretende aceder. Entretanto, invade automaticamente outros computadores que estejam ligados à mesma rede e que ainda não se encontram infetados, funcionando de forma muito rápida. Este programa pode destruir ficheiros, enviar documentos via e-mail, realizar *downloads* e instalar outros tipos de *malware*, ou seja, funciona como porta de entrada (*backdoor*) para o sistema.

Em suma, podemos dizer que o *malware* é um programa que pode surgir de diversas formas e com consequentes funcionalidades, permitindo a monitorização em tempo real de toda atividade do visado, assim como a recolha de dados armazenados no sistema informático infetado, de forma insidiosa, sem o conhecimento do mesmo.

Estes são os tipos de *malware* que consideramos poderem ser mais facilmente utilizados no âmbito da investigação criminal em ambiente digital.

4. A relevância prática no âmbito da investigação criminal

Cientes das novas vulnerabilidades, e com intuito de combater a criminalidade cada vez mais complexa dos crimes perpetrados com recurso às novas tecnologias, os Estados têm vindo a adotar novas medidas, de carácter preventivo e repressivo, para com este tipo delitos, pelo que gradualmente se percebeu a importância de ajustar os "cânones

[29] RAMALHO, David Silva, *Métodos ocultos* (…), op.cit. p. 39.

tradicionais a este admirável mundo novo"[30], atualizando a legislação processual, que passou a abranger esse recurso às novas tecnologias.

Assim, em matéria de recolha de prova, as alterações aos paradigmas inicialmente concebidos têm sido profundas, face à nova realidade, que indisputavelmente suscita novas indagações em matéria de prova. A deslocação da criminalidade do mundo físico para o mundo virtual leva a que ela apenas seja passível de prova com recurso a meios que apenas se encontram armazenados no "cibermundo"[31] e, na verdade, quase todas as infrações penais têm hoje um suporte tecnológico[32].

Atualmente, no nosso ordenamento jurídico, a prova digital encontra-se regulada em três diplomas legais: o CPP, a Lei n.º 32/2008, de 17 de julho (que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas) e a Lei n.º 109/2009, de 15 de setembro, "Lei do Cibercrime" [33]. Contudo, o nosso legislador não esboçou qualquer conceito legal de prova digital na teia legislativa aplicável, pelo que a doutrina e a jurisprudência se têm encarregado de preencher o vazio, apresentando algumas aceções.

Nas palavras de Benjamim Rodrigues, a "prova eletrónico-digital" é, geralmente, definida "como qualquer tipo de informação, com valor probatório, armazenada (em repositórios eletrónico-digitais de armazenamento) ou transmitida (em sistemas e redes informáticas, ou rede de comunicações eletrónicas, privadas ou publicamente acessíveis), sob forma binária ou digital"[34].

As características da prova digital são muito peculiares, distintas das provas físicas, para além de qualquer paralelo de comparação, destacando-se a sua

[30] BARATA, Joana Reis, *O regime jurídico dos conhecimentos fortuitos em ambiente digital: contributo da plane view doctrine à luz da legislação portuguesa*. In: Novos desafios da prova penal / coord. Paulo de Sousa Mendes, Rui Soares Pereira. - Coimbra: Almedina, 2023. p. 347.

[31] BARATA, Joana Reis, *O regime jurídico dos conhecimentos* (…), op. cit. pp. 347-348.

[32] LÓPEZ-BARAJAS Perea, Inmaculada. *«Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos». IDP. Revista de Internet, Derecho y Política*. N.º 24, 2017. pp. 64-76. UOC p. 6. Disponível em https://raco.cat/index.php/IDP/article/view/n24-lopez/420451 (consultado a 12/06/2023).

[33] CORREIA, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público* 139: julho: setembro 2014. p. 30.

[34] RODRIGUES, Benjamim Silva. *Da prova penal: Tomo IV*– Da prova electrónico-digital e da criminalidade informático-digital. Lisboa: Reis dos Livros, 2011. p. 39.

"imaterialidade ou invisibilidade"[35]. A prova digital é "fragmentária, dispersa, frágil, volátil, alterável, apagável e manipulável, invisível e espacialmente dispersa". Por isso se impõe que deva ser "manuseada e transportada com especiais cautelas, sob pena de se hipotecar a sua validade em sede judicial, no que diz respeito à cadeia da custódia da prova"[36].

Para além das especificidades que a prova digital apresenta, também emergem as denominadas medidas anti-forenses[37]. Por um lado, devido ao desenvolvimento da ciência forense digital e, por outro, dada a recrudescente interferência do Estado, no conteúdo das telecomunicações eletrónicas, têm vindo a ser criadas técnicas, mecanismos e programas informáticos com a finalidade de frustrar a deteção, monitorização, prova ou imputação de uma determinada atividade, em ambiente digital, ao seu autor[38].

No entanto, apesar de estas medidas anti-forenses pretenderem beneficiar a privacidade do utilizador, também acabaram por estimular o desenvolvimento de práticas criminosas, a coberto do anonimato providenciado. Neste âmbito, das medidas anti-forenses, analisaremos a anonimização e a encriptação.

Os *softwares* de anonimização são frequentemente utilizados para permitir uma navegação e uma atuação na *internet* anónimas, "insuscetíveis de serem associadas a uma específica proveniência, a um específico sistema informático". Desta forma, o investigador criminal fica tendencialmente impedido de associar uma conduta *online* ao

[35] "Abrimos fisicamente um computador, e encontrámos no seu interior documentos escritos, sons ou filmes sensorialmente apreensíveis" RAMALHO, David Silva, *Métodos ocultos* (…), op.cit. p. 105.
[36] DIAS, Armando Ramos, *O agente encoberto digital: meios especiais e técnicos de investigação criminal*, Coimbra: Edições Almedina, 2021. p. 119.
[37] HARRIS, *Ryan, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problema*.", Elsevier 2006. p. 45. Disponível em https://dfrws.org/presentation/arriving-at-an-anti-forensics-consensus-examining-how-to-define-and-control-the-anti-forensics-problem/ (consultado a 26/2/2023); Citado por 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. out. — dez. de 2013. p. 208. Segundo o autor, as medidas anti-forenses podem ser definidas como "quaisquer tentativas de comprometer a disponibilidade ou utilidade da prova no processo forense. Comprometer a disponibilidade da prova inclui quaisquer tentativas de evitar que a prova venha a existir, de esconder prova existente ou de manipular a prova no sentido de assegurar que a mesma deixe de estar ao alcance do utilizador. A utilidade pode ser comprometida através da obliteração da própria prova ou da destruição da sua integridade"; Na doutrina, o conceito de medidas anti-forenses não é unânime: à partida, elas são designadas por "qualquer técnica, ferramenta de *hardware* ou *software*, que previne ou atrasa a análise forense de um suporte de dados e afeta negativamente a existência, quantidade, autenticidade, ou qualidade da prova obtenível de um computador", RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 151.
[38] RAMALHO, David Silva, *Métodos ocultos* (…), op.cit. pp. 150-151.

respetivo autor, pois o criminoso, com recurso a dados de identificação fraudulentos, oculta a sua origem, ou a dificulta "através de *servidor proxy*, *mix cascades* ou *onion routers*" [39].

Nesta matéria, destaca-se o programa *Tor* [40] (*The onion routers)*, em razão da sua ampla utilização, como meio de anonimização no mundo da cibercriminalidade. Este programa informático foi desenvolvido com a finalidade de garantir a "confidencialidade e inviolabilidade das comunicações"[41], tornando indetetável a localização dos servidores e os seus utilizadores.

O *Tor* é uma ferramenta fundamental no acesso à *Dark Web*, um estrato mais profundo da *Internet*, onde a navegação é livre, tendencialmente anónima, cifrada e potencialmente indetetável[42]; portanto, os conteúdos enviados e recebidos são encriptados, "multiplicando-se os desafios que a investigação criminal já encontra no domínio da Internet"[43]. Neste sentido, o uso de *malware* apresenta-se como uma possibilidade de contorno das dificuldades postas pela encriptação criada pelo do *Tor*, permitindo assim a "identificação e a localização do utilizador do sistema informático"[44], apesar dessas dificuldades.

Retomando a prova digital, não podemos esquecer que ela pode estar "codificada", o que não acontece com a prova tradicional. Isso significa que não pode ser feita a leitura direta da prova cifrada e, portanto, estaríamos perante uma "não-prova"[45].

---

[39] *Idem*, p.153.

[40] Programa informático, que permite a navegação anónima na *Internet* e a navegação em partes da *Internet* normalmente inacessíveis, ou "*Dark Web*. Um lado da *Web* dedicado à cibercriminalidade, (…) cujo acesso é, em geral, limitado àqueles que instalam um software específico". RAMALHO, David Silva, "A investigação criminal na Dark Web", *Revista de Concorrência e Regulação,* ano IV, n.º 14/15 (abril/setembro), 2013. p. 385.

[41] RAMALHO, David Silva, "O *malware* como meio de obtenção de prova em processo penal", *Revista de Concorrência e Regulação,* ano IV, n.º 16 (outubro/dezembro), 2013. p. 212.

[42] RAMALHO, David Silva, "A investigação (…), op. cit. p. 385.

[43] *Idem*.

[44] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 47.

[45] DIAS, Armando Ramos, *O agente encoberto* (…), op. cit. p. 122.

A criptografia[46] possui diversas áreas de atuação, dentre elas a encriptação, que se destina a ocultar o verdadeiro conteúdo da comunicação que se quer transmitir sem ser conhecida por intermediários. No caso da encriptação das comunicações telefónicas, a informação é fornecida pelos fornecedores de serviços, garantindo o acesso ao conteúdo sem obstáculo, mesmo seguindo o protocolo *Global System for Mobile Communication*, GSM, através de uma plataforma própria para os OPC[47]. No que concerne aos *emails*, o tipo de encriptação é distinto, com as comunicações que assentam no Protocolo IP e que correspondem ao *Voice Over Internet Protocolo,* VoIP,[48] bem como as plataformas de comunicação mais comuns, que recorrem à *end-to-end encryptyon,* o que significa que, mesmo que a comunicação passe através de um servidor este não tem acesso ao seu conteúdo apenas o dispositivo recetor tem a chave de desencriptação.[49]

Com efeito, com o desenvolvimento das tecnologias da informação, surgem novos equipamentos informáticos, como os "telefones inteligentes, *smartphones",* com várias aplicações com a técnica de encriptação já predefinida, como é o caso do *WhatsApp*[50] que, consequentemente, permite o envio de mensagens encriptadas de ponta-a-ponta. Assim, a "mensagem é encriptada logo que enviada e apenas o seu destinatário consegue conhecê-la e desencriptar" [51](por ser o detentor da chave secreta), ou seja, torná-la legível. Portanto, a interceção simples do conteúdo de comunicações como estas é manifestamente inútil, pois o recurso à técnica de encriptação dificulta a investigação criminal em ambiente digital.

Para além das medidas anti-forenses já abordadas, surge a ainda uma outra categoria de medidas, levadas a cabo pelos agentes do crime: os ataques contra as perícias

---

[46] A criptografia é o "estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível", de modo a ser reconhecida apenas pelo destinatário, "detentor da chave secreta", o que a torna difícil de ser lida por alguém não autorizado. Desta forma, apenas o "recetor da mensagem pode ler a informação com facilidade". DIAS, Armando Ramos, *O agente encoberto* (…), op.cit. p. 123; ainda há a referir que a criptografia constitui uma concretização prática do "princípio da segurança desde a conceção". Trata-se de um dos princípios gerais do "ciberdireito" que determina que o desenvolvimento das tecnologias assegure aos usuários que os dados não sejam subtraídos por terceiros com fins ilícitos, e que a segurança "deve estar presente desde o momento em que se projeta a tecnologia" CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 43, nota 65.

[47] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 44.

[48] *Idem*, pp. 44-45.

[49] *Idem*.

[50] Para além do *WhatsApp*, surgiu o *Viber*, o *Telegram*, entre outras. DIAS, Armando Ramos, *O agente encoberto* (…), op. cit. p. 123.

[51] DIAS, Armando Ramos, *O agente encoberto* (…), op. cit. p. 123.

forenses. Tratando-se de programas previamente instalados nos sistemas informáticos, com a faculdade de identificarem a execução de programas informáticos relacionados com perícias forenses no sistema, os mesmos ativam mecanismos de agressão às próprias perícias, frustrando a recolha de prova digital.

Assim, atendendo a que o *malware* é um método oculto de obtenção de prova, um software malicioso instalado clandestinamente pelo Estado no sistema informático do suspeito, coloca-se a questão de se saber qual a sua relevância na investigação criminal, ou seja, "se visa responder a alguma necessidade específica"[52], neste âmbito.

Com efeito, em virtude da proliferação das medidas anti-forenses, e da facilidade com que as mesmas podem ser adotadas por utilizadores de conhecimentos técnicos medianos, leva a que o uso do *malware* como meio de obtenção de prova na investigação criminal se revele de extrema importância. Através do *malware,* é possível efetuar a "vigilância na fonte", isto é, aceder aos "dados informáticos *a priori* da encriptação ou *a posteriori* da desencriptação"[53]. Contudo, não podemos olvidar que a introdução do *malware* na investigação criminal suscita conflitos com as finalidades do processo penal.

[52] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 41.
[53] *Idem*, p. 45.

CAPÍTULO II: O EMQUADRAMENTO NOS MÉTODOS OCULTOS DE INVESTIGAÇÃO E O CONFLITO ENTRE AS FINALIDADES DO PROCESSO PENAL

1. Enquadramento nos métodos ocultos na investigação criminal

Ao longo da vigência do CPP, a sociedade mudou, a criminalidade mudou e a propagação das novas tecnologias veio facilitar a prática de ilícitos e, consequentemente, reduziu a possibilidade de deteção dos agentes do crime. Com efeito, como nos diz Anabela Miranda Rodrigues[54], pouco depois da viragem do milénio, o mundo mudou e "nestas coisas da perseguição penal, o processo muda com o mundo, o processo penal mudou".

Nas últimas duas décadas, embora que de forma gradual, temos assistido a uma mudança particularmente notável. Se, no início dos anos 90, a *internet* era um instrumento ou ferramenta de trabalho, apenas "acessível a um nicho muito restrito de pessoas", atualmente cada pessoa transporta nos seus bolsos pequenos computadores, vulgarmente designados por *smartphones*[55] e, por meio deles, consegue ter acesso à informação e à comunicação, superando fronteiras. Através das imagens e da informação, "é-nos permitido visitar lugares distantes, quer no plano virtual, quer no real"[56]. Com efeito, a criminalidade também acompanhou esta mudança, sendo visível a migração de muitos dos delitos para o "ciberespaço".

A nova criminalidade, mais complexa[57], sofisticada e apetrechada de excecionais meios materiais, humanos e internacional, convoca novos desafios à justiça, pelo que os Estados, perante a ameaça instalada na sociedade, procuraram obter novos mecanismos de prevenção e de investigação, consagrando assim a utilização dos novos métodos

[54] RODRIGUES, Anabela Miranda, «A defesa do arguido: uma garantia constitucional em perigo no "admirável mundo novo"», *Revista Portuguesa da Ciência Criminal*, ano 12, n.º 4, out-dez, 2002. p. 550.
[55] DIAS, Armando Ramos, *O agente encoberto* (…), op. cit. p. 11.
[56] BUEKENHOUT, Inês, A Investigação criminal. Desafios presentes e futuros. *Investigação Criminal nº9*, Lisboa, dezembro 2015. p. 12.
[57] VALENTE, Manuel Monteiro Guedes, *Teoria geral* (…), p. 627; CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 49.

ocultos e o recurso aos meios digitais, como instrumentos de combate à corrupção e à criminalidade económico-financeira.

Por outro lado, não podemos esquecer que o recurso a estes métodos excecionais impõem, em regra, a observância de determinados pressupostos, pelo que a necessidade de utilização dos meios ocultos para obter eficácia na perseguição criminal se deve encontrar ajustada à gravidade do crime em causa[58], não bastando, para tal utilização, que o crime seja particularmente difícil, em face dos meios utilizados na sua prática, mas devendo também o grau de lesividade deste ilícito justificar a utilização de um meio também mais gravoso. Para além disso, o recurso a estes meios tem um caráter excecional e não automático, o que se traduz em não estarem disponíveis para qualquer momento, nem para qualquer ilícito, nem sem qualquer critério, e será através da consagração legal destes meios que se delimitará o campo de atuação, no decurso da investigação criminal.[59]

Segundo Costa Andrade, "os métodos ocultos de investigação criminal representam uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto" [60], pelo que se promove que a comunicação se mantenha, de forma aberta e aparentemente normal e inocente, mas, ao mesmo tempo, dirigida à autoincriminação do imputado/suspeito"[61]. Portanto, trata-se de uma ação enganosa e oculta, praticada "nas costas" do suspeito, que, ao continuar a agir com toda a naturalidade, pode até facultar provas para o processo-crime que até poderá desconhecer".[62]

Na verdade, o *malware* pertence a esta categoria doutrinal[63], uma vez que se trata de um *software* instalado de "forma oculta ou furtiva[64]" no sistema informático do investigado, permitindo o acesso a um volume de informações nele incluso, sem que o

[58] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. pp. 204-205.
[59] 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.
[60] ANDRADE, Manuel da Costa, "*Bruscamente no Verão* (…), pp. 104-105.
[61] Segundo o autor, "fazer uso, no processo, de uma conversa telefónica escutada leva à autoincriminação do imputado e, consequentemente, fere os pilares fundamentais da Constituição, sacrificando-se o direito ao silêncio e a liberdade de comunicação. WOLTER, Jürgen, *O inviolável e o intocável* (…), op. cit. p. 161.
[62] CAIRES, João Gouveia. "Métodos Ocultos na Criminalidade Económico-Financeira: Entre a (a)tipicidade e a cumulação." *Revista julgar* n.º 38, 2019. p. 52.
[63] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 50.
[64] WEIBLEN, Fabrício Pinto. *Abertura Tecnológica dos Meios De Obtenção De Prova e o Uso de Software Espião na Investigação Criminal*, 2024. p.25.

visado tenha conhecimento, em razão da "atuação dissimulada ou do desconhecimento intencional por parte dos poderes públicos", ou seja, a ocultação associada a estes métodos é "essencial para a sua eficácia probatória" e as particularidades de que estes meios ocultos se revestem demonstram o alcance da "sua drástica e comprometedora danosidade social".[65]

Estes métodos têm em comum características paradigmáticas não necessariamente cumulativas: i) são ocultados do visado e neutralizam alguns dos seus direitos processuais convencionais, como o direito à não-auto-incriminação; ii) segundo, são abrangentes, pois incidem sobre um número elevado de terceiros e possibilitam a recolha de informações, perscrutando qualquer fase da vida e não se limitando à fase de investigação; iii), anulam também o direito de certas testemunhas a não prestarem declarações; iv) permitem recolher informações sem qualquer cuidado ou atenção à intimidade ou à fiabilidade da comunicação[66].

Em bom rigor, os recursos aos métodos ocultos restringem um leque de direitos fundamentais, e também apresentam uma certa deslealdade, tendo em conta que restringem a liberdade ao visado para que, "querendo, possa definir os limites da sua ação"[67]. Ademais, como refere Manuel da Costa Andrade,[68] esses recursos acabam por deslocar uma maior importância para a fase de inquérito, e é nesta fase que se alcançam os resultados das investigações ocultas, o que leva a que o juiz se veja "desarmado"[69], em face do MP e dos OPC. Assim, é concedida ao Estado "uma extensa permissão de

[65] ANDRADE, Manuel da Costa, *Bruscamente no Verão* (…), op. cit. p. 106.

[66] ALBRETCH, Hass-Jorg, "vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos". AA.VV. Que Futuro Para o direito Processual Penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal. Coimbra: Coimbra Editora. 2009.p. 726 -727; RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 209.

[67] CAIRES, João Gouveia. "Métodos Ocultos na Criminalidade Económico-Financeira: Entre a tipicidade e a cumulação." *Revista julgar* n.º 38, 2019. p. 51; CAMPOS, Juliana Filipa Sousa, *O Malware* (…), op. cit. p. 51.

[68] ANDRADE, Manuel da Costa. *Bruscamente no Verão* (…), op. cit. p. 107; RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 209.

[69] O recurso sistemático aos meios ocultos de investigação induz e provoca tropismos na dinâmica processual. Pois, o cento de gravidade das decisões tende a deslocar-se do julgamento (publico) para os resultados das investigações ocultas. ANDRADE, Manuel da Costa. *Bruscamente no Verão* (…), op. cit. p.107.

atuação", colocando em causa o estatuto processual do arguido e, consequentemente, corroem-se os fundamentos do Estado de Direito Democrático[70].

Por tudo o que acima se expõe, é determinante que o processo penal acompanhe a evolução do Mundo e das novas tecnologias da comunicação, e que venham a ser previstos novos métodos de obtenção de prova que se coadunem com a atualidade. Contudo, estes novos meios devem ser regulados criteriosamente, uma vez que lesam direitos fundamentais. De facto, ainda que estejamos diante da alta criminalidade, "que destrói ou, pelo menos, coloca em causa o Estado de Direito Democrático"[71], o combate a esta criminalidade não se pode conformar com uma total discricionariedade dos meios empregues.

Ainda nas palavras deste autor, a utilização destes métodos vai além da lesão dos direitos de cariz adjetivo processual (ou seja, o direito ao silêncio, a recusa de depoimento, entre outros), também implicando, no plano material substantivo, a sujeição "à passagem de um espectro de bens jurídicos ou de direitos fundamentais como privacidade, intimidade palavra imagem, sigilo profissional inviolabilidade do domicílio, segredo de Estado, sigilo das telecomunicações, confidencialidade e integridade dos sistemas técnicos internacionais ou autodeterminação informacional.[72]

Todavia, a integração do *malware* no âmbito dos métodos ocultos de investigação, responde às exigências de combate à criminalidade contemporânea, que é caracterizada por uma "delinquência não convencional", sob múltiplas manifestações, evidencia um conflito inescapável entre as finalidades do processo penal[73].

---

[70] CAIRES, João Gouveia. "Métodos Ocultos na Criminalidade Económico-Financeira: Entre a tipicidade e a cumulação." *Revista julgar* n.º 38, 2019. pp. 51-52.

[71] HENRIQUES, Marco Ribeiro. Ações Encobertas, para fins de investigação criminal. A dicotomia entre o agente infiltrado e agente provocador. *Revista Jurídica UNIGRAN*. Dourados, MS | v. 18, n.º 35: jan./jun.2016. p. 94.

[72] *Idem*, pp 106-107.

[73] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op.cit. p. 52; SOUSA, Paulo Pinto de "Ações encobertas: meio enganoso de prova? agente infiltrado e agente provocador. Outras questões.", *Revista do CEJ* 2.º semestre, n. º14, 2010. p. 231.

2. O conflito entre as finalidades do processo penal

2.1. A descoberta da verdade material e a realização da justiça

É sabido que a abertura das portas do mundo físico para o infindável mundo digital apresenta novos desafios, no que diz respeito à adaptação dos sistemas jurídicos à nova realidade, o que se reflete na lógica do sistema processual penal.

São três as finalidades apontadas ao processo penal: a realização da justiça, a descoberta da verdade material, autónomas entre si, e a proteção dos direitos fundamentais das pessoas, face ao Estado[74] [75]. Contudo, estas finalidades, não são integralmente conciliáveis, pelo seu "caráter irremediavelmente antinómico e antitético"[76]. Segundo o ensinamento de Figueiredo Dias, a via de superação da impossibilidade de harmonização integral destas finalidades só pode ser percorrida se se "operar a concordância prática das finalidades em conflito; de modo que cada uma se salve, em cada situação, o máximo conteúdo possível, otimizando os ganhos e minimizando as perdas axiológicas e funcionais, com o limite da intocável dignidade da pessoa humana"[77].

Desta forma, a problemática da prova apresenta-se como um campo onde claramente se observa este conflito. Daí que, quando se "preveem determinados meios de obtenção de prova, sejam estes ocultos ou abertos", ressalta um conflito entre a descoberta da verdade material, a realização da justiça e a proteção perante o Estado dos direitos fundamentais das pessoas.[78] Também, quando se proíbem determinados meios de obtenção de prova e, depois, a subsequente valoração de provas obtidas por tais meios,

[74] Do arguido e, também, de outras pessoas.
[75] ANTUNES, Maria João. *Direito Processual Penal*, 3ª Edição. Almedina, 2021. p. 18.
[76] Dias, Jorge de Figueiredo, Direito Processual Penal: Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por Maria João Antunes, Coimbra: Secção de textos da Faculdade de Direito da Universidade de Coimbra, 1988-1989. p. 25.
[77] DIAS, Jorge de Figueiredo, Direito Processual Penal: Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por…, op. cit. p. 25; ANTUNES, Maria João, *Direito Processual Penal* (…), op. cit. p.19.
[78] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p .53. ANTUNES, Maria João, *Direito Processual Penal* (…), op. cit. p. 14.

observa-se o mesmo conflito entre a proteção dos direitos fundamentais das pessoas e a descoberta da verdade material e da realização da justiça, sob outra perspetiva.[79]

Assim, com a introdução de um novo meio de obtenção de prova, pressupõe-se a descoberta da verdade material, que é, no processo penal, um dever ético e jurídico,[80] pretendendo-se que a prova seja mais abrangente e conducente à concreta realização da justiça, "componente essencial do princípio do Estado de direito" [81].

O recurso ao novo meio de obtenção de prova do *malware*, com vista à descoberta da verdade, em circunstâncias que assim justifiquem, e em virtude dos obstáculos e dificuldades com que a investigação criminal se depara, nos dias de hoje, face aos avanços da tecnologia, tornar-se-ia vantajoso, pois permitiria a obtenção de material probatório determinante à dita descoberta da verdade, sobretudo quando estamos em face de crime organizado e de terrorismo. "[82]

Todavia, devemos ter presente que "os meios ocultos de obtenção de prova e as novas tecnologias de comunicação representam uma restrição aos direitos, liberdades e garantias fundamentais pessoais", pelo que o recurso a eles para combater a criminalidade organizada e estruturada nacional, regional e internacional, requer a adoção de medidas excecionais e uma rigorosa legislação adequada, de acordo com o "quadro jurídico-constitucional legítimo, válido, vigente e efetivo sob pena de negarmos o Estado constitucional democrático"[83].

3. As proibições de prova como limite à descoberta da verdade

3.1. Proibições da prova

É inquestionável a oscilação dos "sistemas probatórios em matéria penal", quanto à aspiração à descoberta da verdade material e ao respeito pela legalidade. É neste

[79] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. pp. 53-57; ANTUNES, Maria João. *Direito Processual Penal*, 3ª Edição. Almedina, 2021. p. 14.
[80] Ac. TRL 141/18.8JELSB-A. L1-5, de 11/09/2018. Relator José Adriano.
[81] *Idem*.
[82]SOUSA, Paulo Pinto "*Ações Encobertas*… op. cit. p .231; CAMPOS, Juliana Filipa, *O malware* (…), op. cit. pp. 54-55.
[83] VALENTE, Manuel Monteiro Guedes, Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias". *Revista Brasileira De Direito Processual Penal*, 2017. p. 481.

entrelaçar de aspirações conflituantes que "a legalidade dos meios de prova, bem como as regras gerais de produção de prova e as chamadas 'proibições da prova', são condições de validade processual da prova e, por isso, critérios da própria verdade material"[84].

As proibições de prova são autênticos limites à descoberta da verdade material, "barreiras colocadas à determinação do objeto do processo". A regra sobre a produção da prova configura diversamente, meras prescrições ordenativas da produção de prova, cuja violação não poderia acarretar a proibição de valorar como prova.[85]

Elas surgem "como uma das instituições mais marcantes do novo ordenamento processual, erigido a partir dos alicerces sediados diretamente na Constituição de 1976"[86], e são um "dos meios de que se serve a lei para proteger os cidadãos contra ingerências abusivas nos seus direitos, no âmbito de uma investigação criminal"[87].

A base legal das proibições de prova determina que estas são provas obtidas em violação dos direitos constitucionalmente garantidos, através dos quais a Constituição estabelece verdadeiras normas processuais a ser respeitadas[88].

Como referido, o *malware* será instalado sub-repticiamente num sistema informático, de forma presencial ou remotamente, com a finalidade de serem extraídos dados, ou de monitorização em tempo real, sem o conhecimento do visado, podendo a sua propagação ocorrer através de um comportamento voluntário, inadvertido do utilizador ou de formas que não carecem dessa subsequente intervenção humana.

Sucede pois que, agindo de espontânea vontade e por desconhecimento, pode o visado proceder à instalação do *malware,* por exemplo quando carrega num *link*, num anexo de *email* ou num *site*, por estes se apresentarem de forma inofensiva,

---

[84] SILVA, Sandra Oliveira e. "Legalidade da prova e provas proibidas". *Revista Portuguesa de Ciência Criminal*, Ano 21, n.º 4, out./dez. 2011. p. 545.
[85] Ac. STJ Proc. N.º 07P4553 – de 20/02/2008. Relator Armindo Monteiro. Consultado (consultado em 18/01/2024)
[86] ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal*, 2.ª impressão, Gestlegal Editora, 2022. p. 13.
[87] SILVA, Germano Marques da. *Curso de Processo Penal* Vol. II, 5.º Edição revista e atualizada, Verbo, 2011. p. 173.
[88]ANDRADE, Manuel da Costa, *Sobre as Proibiçõ*es (...), op. cit. pp.13-14.

empreendendo assim uma conduta que, equivocadamente, o conduzirá à instalação de um programa, e assim comprometendo "a sua liberdade, vontade de decisão"[89].

Ora, a ser assim, poder-se-ia suscitar a questão de se não estaríamos no âmbito dos meios de prova enganosos, conforme decorre do artigo 126º, n.º2 do CPP, dando lugar a provas nulas, de acordo com o disposto no artigo 32º, n.º 8 da CRP, que prescreve que "são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações", mandamento constitucional que é, por sua vez, replicado no artigo 126.º do CPP. Desta forma, observa-se uma tensão entre as finalidades da realização da justiça e da descoberta da verdade material e a finalidade de proteção perante o estado dos direitos fundamentais das pessoas[90].

Contudo, a proibição de prova tem como finalidade a garantia do respeito pelos direitos fundamentais e representa uma barreira de "limites intransponíveis" à obtenção de prova a "todo o preço", que se traduzem nos limites da descoberta da verdade material[91]. Assim, estando na presença de um meio de obtenção de prova que "pode ser reconduzido aos meios enganosos, deparamo-nos com um limite à descoberta da verdade"[92].

Portanto, releva que esclareçamos "o que se entende por meio enganoso", estabelecendo um limite a esta conceptualização, por forma a podermos compreender se o *malware* é realmente um meio de prova enganoso, conforme dispõe o artigo 126º, n.º 2 do CPP, ou se, eventualmente, é antes reconduzível aos "métodos astuciosos de obtenção de prova"[93] .

Sabemos que os meios enganosos se encontram num "domínio indefinido e inseguro e onde, por isso, sobem de tom as dificuldades das proibições da prova"[94]. Contudo, aqui pretendemos apenas averiguar se o *malware* pode ser integrado, ou não,

[89] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 75.
[90] ANTUNES, Maria João, *Direito processual* (…) op. cit. p. 18.
[91] ANDRADE, Manuel da Costa, *Sobre as Proibições*…op. cit. p. 123.
[92] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 75.
[93] *Idem*, p. 76
[94] ANDRADE, Manuel da Costa, *Sobre as Proibições* (…), op. cit. p. 241.

no âmbito "meio enganoso "à luz do critério da relevância do engano no crime de burla, artigo 217º do CP"[95].

Se o utilizador instalar o *malware* no seu sistema informático, induzido em erro, exterioriza uma conduta que ignora determinados factos, que, por sua vez, podem repercutir consequências penais, o que nos leva a crer que o visado está em erro, pois se observa uma "representação da realidade, não correspondente à realidade objetiva". Desta forma, para que um meio de prova possa ser considerado enganoso deve "o agente investigador, através de factos ou atos concludentes", criar no arguido uma convicção errónea, determinante da prática do ato, da prova, que o prejudica a si ou a terceiros, tornando-o numa testemunha[96].

Portanto, na perseguição criminal, para a descoberta da verdade, a AJ ou os OPC, quando recorrem ao uso do *malware*, suscitam no utilizador do sistema informático uma "convicção errónea"[97]. Não podemos, porém, afirmar que o facto de ter sido enviado o *malware* seja gerador da prática de um crime ou para a prestação da prova, isto é, não se trata de o utilizador ter instalado um programa malicioso (ainda que sem conhecimento) que permite concluir que este usou o sistema informático de forma distinta para a prática de crimes, ou para permitir o acesso a dados informáticos, que "estejam armazenados ou que venham a ser produzidos de conteúdo incriminatório".

No entanto, pode acontecer o utilizador pretender armazenar dados informáticos ou realizar uma atividade, não sendo o *malware* que isso determina, pelo que se torna difícil confirmar e desafiador estabelecer um nexo causal entre a instalação do *malware*, sob convicção errónea, e a prática do crime, ou da sua prova. Assim sendo, podemos considerar que o *malware* não se enquadra nos meios de prova enganosos, de onde que, nos termos do artigo 126º, n.º 2 do CPP não é um método proibido de prova.

Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, sem o consentimento do respetivo titular. Ora, a instalação do *malware* pode representar a intromissão da vida privada, no domicílio e

[95] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 76.
[96] *Idem*.
[97] *Idem.*

nas telecomunicações, não relevando para o efeito o consentimento prestado aquando da instalação, uma vez que, mesmo existindo, não foi realizado de forma livre e esclarecida e, a ser assim, a prova obtida ter-se-ia de enquadrar nos métodos proibidos de prova, conforme o artigo 126º, n.º 3 do CPP.

3.2. O princípio *nemo tenetur se ipsum accusare*

O princípio *nemo tenetur se ipsum accusare* é muito relevante, no processo penal português, pois é um dos limites à descoberta da verdade material, traduzindo-se na garantia do direito de defesa atribuída ao arguido[98], sendo que garante o direito à não-autoincriminação.

O direito à não-autoincriminação não se encontra expressa e diretamente consagrado no texto constitucional[99], nem na CEDH[100], mas é "amplamente reconhecido" no nosso ordenamento. Constitui um corolário da tutela de valores ou direitos fundamentais, com direta consagração constitucional[101], e é, na generalidade das vezes,

[98] Com "projeção normativa e prática jurídica dos dispositivos constitucionais atinentes aos da dignidade humana, da liberdade geral da ação ou do direito ao livre desenvolvimento, a liberdade de declaração não é um exclusivo do arguido", ela assiste igualmente a outros sujeitos processuais, nomeadamente à vítima e às testemunhas. ANDRADE, Manuel da Costa, *Sobre as Proibições* (…), op.cit. pp. 126-127.

[99]No que respeita aos fundamentos constitucionais do princípio *nemo tenetur*, a doutrina divide-se em duas correntes principais: uma que atribui fundamento material ou substantivo ao *nemo tenetur*, e o relaciona com alguns direitos fundamentais, como a dignidade humana (artigo 1º CRP) ou, ainda, os direitos à integridade pessoal e ao desenvolvimento da personalidade (artigos 25º e 26º CRP); e outra corrente, a prevalecente na doutrina e jurisprudência[99], que lhe atribui um fundamento processual baseado nas garantias processuais reconhecidas ao arguido na Lei fundamental, como o princípio do processo equitativo e princípio da presunção da inocência, (artigos 20º, n.º 4 in fine e 32º, n.º 2, e n.º8º da CRP, respetivamente) Jorge de Figueiredo Dias/ Manuel da Costa Andrade"Poderes de Supervisão…", op. cit. pp. 41-42; RAMOS, Vânia Costa, "Corpus Juris 2000 - Imposição ao arguido de entrega de documentos para prova e *nemo tenetur se ipsum accusare*" – Parte II, in *Revista do Ministério Público*, Lisboa, Ano 28, n.º 109 (Janeiro-Março 2007). pp. 62-63.

[100] A jurisprudência do Tribunal Europeu dos Direitos do Homem tem, no seu centro, a ideia de que o "direito ao processo equitativo", assegurado pelo artigo 6º, n.º 1, da Convenção, integra expressa ou implicitamente, um conjunto de diferentes elementos, entre os quais o direito ao silêncio e o direito à não-autoincriminação. Segundo o TEDH, apesar de não expressamente mencionados no artigo 6º da Convenção, o direito ao silêncio e o direito à não-autoincriminação constituem padrões (*standards)* internacionais que se situam no coração da noção de "processo equitativo" (*fair procedure*), tendo, na sua razão de ser, a ideia de proteção do acusado contra o exercício impróprio de poderes coercivos parte das autoridades, enquanto condição essencial ao acautelamento contra o perigo de adulteração da justiça e, neste sentido, de proteção da própria realização plena do espírito do art. 6.º da Convenção. COSTA, Joana, "O princípio *nemo tenetur* na Jurisprudência do Tribunal Europeu dos Direitos do Homem", *Revista do Ministério Público 128*: outubro/ dezembro 2011. p. 118.

[101] Acórdão Tribunal Constitucional, nº418/2013, de 15 de julho de 2013, relatora Conselheira Catarina Sarmento e Castro. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20130418.html (Consultado em 5/11/2023).

reconduzido às garantias processuais consagradas nos artigos 20º n.º 4, e 32º, n.ºs 2 e 8, da Lei Fundamental[102].

Por outro lado, a jurisprudência do Tribunal Europeu dos Direitos Humanos, baseada no artigo 6.º, n.º 1, da CEDH, tem vindo intensificar consideravelmente o *nemo tenentur*. São várias as situações consideradas possíveis de proteção pelo *nemo tenetur* que, a nível do TEDH, têm a mesma proteção e, portanto, são ocorrências em que estão em causa a dignidade humana e a autodeterminação do arguido[103]. Assim, ainda que este princípio não se encontre vertido em nenhum diploma, a nível prático vigora a regra da aceitação e respeito pela sua aplicabilidade em todas as suas vertentes[104], mesmo no caso da existência de divergências doutrinárias.

Ao arguido é concedida, salvas as restrições previstas na lei, o direito de não contribuir para a própria autoinculpação, isto é, não ver postergado ou comprimido o seu direito e, portanto, a prerrogativa de "não prestar declarações sobre a factualidade que lhe é imputada"[105], assim eventualmente não colaborando na descoberta da verdade. Tal circunstância decorre do seu estatuto processual, fundado num incondicional respeito pela sua vontade, com reflexos em matéria de prova[106].

Esta liberdade concedida pode-se analisar numa dupla dimensão: pela positiva, que se traduz na possibilidade de abrir ao arguido o mais irrestrito "direito de intervenção e de declaração, em abono da sua defesa"; e pela negativa, a liberdade de declaração do

---

[102] CORREIA, Hélder Santos e NEVES, Rita Castanheira. A Lei do Cibercrime e a colaboração do arguido no acesso aos dados informáticos. *Atualidade Jurídica Uría Menéndez*, Lisboa, n.º 38, p. 146 e ss., 2014 disponível.https://www.uria.com/documentos/publicaciones/4377/documento/fp02.pdf?id=5591. (Consult ado 5/11/2023).

[103]MENDES, Paulo de Sousa. *Lições de Direito Processual Penal*. Coimbra: Almedina. 2020. pp. 209-215.

[104] Direito ao silêncio e direito de não facultar meios de prova.

[105] A "faculdade reconhecida ao arguido de não se pronunciar sobre os factos que lhe são imputados, diferentemente do que sucedia nos processos regidos pelo princípio do inquisitório em que as declarações obrigatórias do arguido, *maxime* a confissão forçada, tendem a convertê-lo em instrumento da sua própria condenação. O direito ao silêncio tem vindo a ser reconhecido pela legislação processual penal da maioria dos ordenamentos jurídicos dos Estados de direito modernos, encontrando também consagração expressa em instrumentos jurídicos internacionais (cf. o artigo 6.º da Convenção Europeia dos Direitos do Homem e artigo 14.º do Pacto Internacional sobre Direitos Civis e Políticos). Já o segundo, entendido como direito a não contribuir para a própria incriminação, impede a transformação do arguido em meio de prova por via de uma colaboração involuntária obtida com recurso a meios coercivos ou enganosos. Existe uma ligação íntima entre os dois direitos, desde logo porque, não sendo reconhecido ao arguido o direito a manter-se em silêncio, este seria obrigado a pronunciar-se e a revelar informações que poderiam contribuir para a sua condenação". Ac. TC n.º 298/19, de 15/5/2019, Relator: Conselheiro Pedro Machete. https://www.tribunalconstitucional.pt/tc/acordaos/20190298.html, (consultado em 19/04/2024).

[106] ANTUNES, Maria João, *Direito Processual Penal* (…), op. cit. p. 53-54.

arguido "ganha a estrutura contra o Estado, vedando todas as tentativas de obtenção, por meios enganosos ou por coação, de declarações autoincriminatórias[107]".

Desta forma, o arguido não pode ser fraudulentamente induzido nem coagido a contribuir para a sua condenação, acarrear ou oferecer meios de prova contra si (a sua defesa), seja em relação aos factos relevantes para a questão da culpabilidade, seja em relação à medida da pena, tal não obstando, no entanto, a que o arguido tenha o dever de colaboração, sendo assim necessário garantir que "qualquer contributo do arguido, que resulte em desfavor da sua posição, seja uma afirmação esclarecida e livre de autorresponsabilidade"[108].

O princípio ora focado representa um mecanismo de defesa para o arguido, podendo dele dispor em circunstâncias especificas, e lhe permitindo a defesa em situações em que, por meio de declarações, se pudesse prejudicar. Portanto, surge como limite à descoberta da verdade, pois, "ainda que o arguido detenha elementos probatórios",[109] não fica compelido a os facultar para o processo penal.

De acordo com exposto, a relação entre o uso investigativo do *malware* e o princípio *nemo tenetur* é de incompatibilidade, se considerarmos que é o próprio visado que inadvertidamente procede à instalação do programa insidioso, permitindo assim o acesso às suas próprias declarações, aos dados informáticos em tempo real ou armazenados, ou até mesmo às atividades autoincriminatórias. Desta forma, estaria o próprio visado em colaboração involuntária com a administração da justiça, tendo em conta que o material recolhido pode ser utilizado contra si no processo penal, ao invés do pretendido.

Assim, a obtenção de declarações autoincriminatórias com recurso a *malware*, no âmbito das investigações levadas a cabo pelos OPC, em que o utilizador desconhece que está a ser monitorizado, leva-nos a crer que o princípio do *nemo tenetur* é violado, tendo em conta que é retirado ao visado o direito ao silêncio, uma vez que ele continua a comunicar de forma espontânea e ingénua (inocente), podendo revelar conteúdos que o autoincriminam.

---

[107] ANDRADE, Manuel da Costa, *Sobre as Proibições*…op. cit. p. 127.
[108] *Idem*, p. 121.
[109] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op.cit. p. 70.

Contudo, importa a todo o momento ter presente que este princípio não é um princípio absoluto pois, em bom rigor, pode ser restringido, quando a lei assim o determine, e desde que sejam constatáveis os pressupostos dos princípios da legalidade e da proporcionalidade, plasmados no artigo 18º, n.º 2 da CRP, o que requer uma análise precisa dos conflitos em causa e, nesse caso, uma vez atendidos os requisitos, poder-se-ia obter prova de conteúdo autoincriminatório com recurso a *malware*.

O direito ao silêncio não é sinónimo do princípio *nemo tenetur*, mas sim seu corolário e ambos servem a proteção do arguido. O direito à não autoincriminação confere ao arguido a prerrogativa de não colaborar, no decurso da investigação, pelo que o recurso ao *malware* por parte de AJ ou OPC, viola claramente esse direito de não facultar provas ou declarações que o podem incriminar, tendo em conta que desconhece estar a ser monitorizado, e desde logo compromete a sua vontade em manter o silêncio.

Como referido, o direito ao silêncio é um corolário do *nemo tenetur* que se alonga para além das declarações autoincriminatórias: Quando o arguido é obrigado a colaborar, respondendo com a verdade, entregando documentos ou se sujeitando a exames, há claramente uma restrição do direito de não facultar provas contra si próprio, o que faz com que estas restrições, a terem de existir, careçam de previsão legal[110].

A jurisprudência do TEDH tem considerado que o princípio "não se estende ao uso, em processo penal, de elementos obtidos do arguido por meio de poderes coercivos, mas que também existam independentemente da vontade do sujeito, *inter alia*, documentos adquiridos na execução do mandado de busca, colheitas por expiração, colheitas de sangue, de urina, ou de tecidos corporais, para análise de ADN"[111].

Desta forma, podemos entender que o recurso ao *malware* para obtenção de dados informáticos não requer o uso de poderes coercivos, mas limita a vontade do visado que, de forma para si desconhecida coopera com a investigação, dando a esta o acesso a declarações e a outros dados informáticos.

[110] MENDES, Paulo de Sousa. *Lições de Direito Processual Penal.* Coimbra: Almedina, 2020. p. 210.
[111] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p.73.

Como qualquer outro meio oculto de obtenção de prova o uso do *malware* requer uma análise ponderada, não podendo ser utilizado numa vigência irrestrita e sem qualquer limitação e, portanto, torna-se necessária a criação de uma lei própria.

4. A restrição de direitos fundamentais

Cabe ao Estado de Direito Democrático, de entre as suas finalidades, encontrar o "equilíbrio entre o interesse da prossecução estatal e o interesse da liberdade dos cidadãos", em busca da verdade material[112]. No entanto, "há espaços que, em princípio, o Estado não pode adentrar, e esses espaços chamam-se direitos fundamentais"[113], que se encontram protegidos pela Constituição. Contudo, pode o Estado se ver obrigado a adentrar esses "espaços individuais protegidos", mas, para que tal aconteça, necessitará de uma "justificação especial"[114].

Em tal justificação, devem constar "três pressupostos", concernentes a todos os "direitos fundamentais a serem respeitados": um, de natureza formal, que se traduz na existência de um fundamento legal; e outros dois, de natureza material, que consistem em que a intervenção não afete o núcleo dos direitos fundamentais ("chamados conteúdo essencial ou de dignidade") e que seja proporcional"[115].

No anterior ponto estabelecemos, pois, que o uso de métodos ocultos na investigação criminal constitui uma das formas de resposta aos desafios erigidos pela nova criminalidade, e que estes "modernos métodos de investigação revolucionaram o nosso direito processual penal"[116], reacendendo a problemática da prova, e criando desafios à justiça[117].

Por seu turno, o *malware* é um desses meios ocultos de obtenção de prova que atentam e contendem com um leque de direitos fundamentais. De facto, uma vez

---

[112] WOLTER, Jürgen, *O inviolável e o intocável no processo penal* – Reflexões sobre a dignidade humana, proibições de prova, proteção de dados e separação informacional de poderes diante da persecução penal, São Paulo, Marcial Pons, 2018. p. 109.
[113]GRECO, Luís; Gleizer, Orlandino. A infiltração *online* no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal,* Porto Alegre, vol. 5, nº 3, p. 1485.
[114] *Idem*, p. 1485.
[115] *Idem.*
[116] CAIRES, João Gouveia. "Métodos Ocultos na Criminalidade Económico-Financeira: Entre a tipicidade e a cumulação." *Revista julgar* n.º 38, 2019. p. 52.
[117] VALENTE, Manuel Monteiro Guedes, *Teoria geral do direito policial*, 6ª edição, Almedina, 2019. p. 627.

instalado no sistema informático do suspeito, este meio proporciona o acesso a uma grande quantidade de informação, tanto de dados armazenados, como dos produzidos em tempo real, o que se torna particularmente intrusivo, uma vez que o *malware* opera como instrumento potencialmente revelador de vários aspetos ligados ao desenvolvimento da personalidade[118] e, simultaneamente, a restrição "do direito à integridade e confidencialidade dos sistemas informáticos"[119]. No entanto, este direito só é restringido "se houver a expectativa" de que o suspeito "utiliza aquele sistema informático"[120].

Com efeito, a questão da infiltração do Estado, de forma oculta e remota, começou a ser discutida pelos tribunais alemães[121]. Foi com o Acórdão do Tribunal Constitucional Federal Alemão, de 27 de fevereiro de 2008 [122], que veio a ser criado o direito à confiabilidade e integridade dos sistemas técnico-informáticos, com a finalidade de proteger contra o acesso oculto aos sistemas informáticos investigados e toda a informação constante nestes, independentemente do conteúdo armazenado, dos dados transmitidos em tempo real e de se o sistema informático "se encontra fixo num determinado lugar, ou se é um dispositivo móvel"[123].

Este direito surgiu aquando da introdução do §5.2 (11)[124] na Lei de Proteção da Constituição da Renânia do Norte-Vestefália, em 20 de dezembro de 2006, uma norma que veio conferir à *Bundesamt für Verfassungsschutz* (entidade responsável pela proteção

[118] "é restringido o direito à integridade e à confidencialidade dos sistemas técnico-informáticos. Direito, este, criado pela jurisprudência alemã". CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 57.
[119] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 55.
[120] *Idem*, pp. 57-58.
[121] A questão começou a ser discutida pelos tribunais alemães em 2006, sendo que, inicialmente, "houve tentativas de utilização desse método oculto de investigação com base em aplicações extensivas ou mesmo analógicas de três normas do ordenamento jurídico alemão: aquelas que autorizavam a apreensão de objetos com finalidade investigativa (§94, Código de Processo Penal alemão – *Strafprozessordnung*, StPO), a de busca domiciliar (§ 102 StPO) e a do monitoramento de telecomunicações (§ 100a StPO)". GRECO, Luís; GLEIZER, Orlandino. A infiltração online, no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1488.
[122] Acórdão BverfG, 1 BvR 370, 595/07, de 27 de fevereiro de 2008, disponível em: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, consultado em 26/11/2023.
[123] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 57.
[124] A norma determina que a autoridade, para proteção da Constituição, pode aplicar as seguintes medidas: a monitorização secreta e outro reconhecimento da Internet, como, em particular, a participação encoberta nos seus meios de comunicação e de pesquisa e o acesso secreto a sistemas informáticos, envolvendo a instalação de meios técnicos. Na medida em que tais medidas constituam uma ingerência no segredo da correspondência, ou das telecomunicações, ou seja, equivalham a tal ingerência, em termos de natureza e gravidade, a norma será apenas admissível sob as condições do artigo 10 da Lei Fundamental". Nota, RAMALHO, David Silva, *Métodos Ocultos de Investigação* (…), op. cit. p. 217.

da Constituição) o acesso secreto a sistemas informáticos, com recurso à exploração de vulnerabilidades técnicas, para a instalação de *malware.*[125]

O Tribunal alemão começou por analisar o problema à luz de três direitos fundamentais: o direito à privacidade da correspondência, do correio e das telecomunicações; também o direito à inviolabilidade do domicílio e o direito à autodeterminação informacional[126].

Assim, a primeira conclusão extraída pelo BVerfG foi a de que os direitos fundamentais, dos artigos 10 e 13 GG, que conferem o direito à proteção do sigilo das telecomunicações e do domicílio, não seriam suficientes para proteger o individuo contra o acesso aos seus sistemas informáticos[127].

O tribunal observou que o artigo 10 GG, referente ao direito ao sigilo das telecomunicações, protege a telecomunicação privada, garantindo a confiabilidade da comunicação entre indivíduos distantes entre si, mas, não protege os dados guardados nos sistemas informáticos nem o monitoramento (rastreamento/vigilância) destes[128].

O artigo 13 GG, tem como objetivo garantir a proteção da inviolabilidade do domicílio, "com vista à dignidade humana e ao interesse no desenvolvimento da personalidade", ao se tratar de um espaço físico elementar de vida. Pretendendo-se proteger o domínio espacial no qual a vida privada se desenvolve".

Segundo a visão do BVerfG, esse direito fundamental não seria pertinente, "pois o seu objeto de proteção seria uma componente espacial do âmbito privado, que não seria interferida, caso uma intervenção ocorresse a partir de fora do domicílio, ou caso a situação do dispositivo em questão (um *laptop* ou um *smartphone*) não fosse reconhecível durante a investigação. A utilização de uma conexão do dispositivo com a *internet*, ou com um outro computador, também não interferiria no domínio espacial da vida privada"[129].

[125] *Idem*, pp. 217-218.
[126] RAMALHO, David Silva, *Métodos Ocultos de Investigação* (…), op. cit. pp. 217-218.
[127] GRECO, Luís; GLEIZER, Orlandino. A infiltração *online* no processo penal (…), op. cit. p. 1491.
[128] *Idem*, p. 1492.
[129] *Idem.*

Foi nesta senda que o BVerfG entendeu que, para fazer frente aos especiais perigos ao livre desenvolvimento da personalidade, na era digital, ligados ao uso de "computadores como dispositivos individuais, ou como sistemas interconectados", seria indispensável a criação de um outro direito fundamental, derivado do direito geral da personalidade.

Assim, no nosso entender, a lei constitucional portuguesa pode acolher este direito, no âmbito do direito ao livre desenvolvimento da personalidade, de acordo com a previsão do artigo 26º n. º1 da CRP, que comporta em si uma "dimensão de liberdade" a qual não permite a "ingerência dos poderes públicos ou poderes privados dotados de poderes públicos". Porém, o uso de *malware* pode abranger indiscriminadamente todos os dados armazenados, não armazenados e captados em tempo real, pelo que consideramos que fica afetado o direito "a não ser expiado", aquando da monitorização do sistema informático. Para além de que fica afastada qualquer possibilidade de arbítrio sobre "quando e dentro de que limites os seus dados pessoais podem ser revelados"[130], o que conduz à restrição do direito á autodeterminação informacional, previsto nos artigos 26º, n.º 1 e 35º da CRP.

Repare-se que o uso do *malware* pode também restringir o direito à reserva da intimidade da vida privada e familiar, não apenas pelo acesso ao sistema informático, mas também pela recolha de provas externas àquele, aquando da ativação do *hardware*. Assim sendo, presencia-se a "devassa daquela área" e a violação de outros direitos fundamentais, nomeadamente do direito à palavra, quando o microfone é ativado, ou do direito à imagem quando a câmara é ligada, artigo 26º, n.º 1 da CRP.

Desta feita, por se encontrarem vários aspetos relacionados com o "desenvolvimento da personalidade e o livre exercício da mesma", e tendo em conta a confiança que a pessoa detém, ao acreditar que tais dados não são acedidos por outros, o enquadramento será feito na denominada "esfera mais íntima da intimidade"[131], o que

[130] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo", in *A Inteligência Artificial no Direito Penal* (coord. Anabela Miranda Rodrigues), Coimbra: Almedina, 2020. p. 130.

[131] Do "ponto de vista constitucional, o direito à inviolabilidade do domicílio e da correspondência tutela do direito à intimidade pessoal, põem em relevo que o domicílio se configura como uma «projeção espacial da própria pessoa e a correspondência como extensão da própria pessoa». Assim sendo, o direito à inviolabilidade do domicílio é um *direito à liberdade da pessoa*. É, por isso, «... a Constituição considera a 'vontade', o 'consentimento' da pessoa (nº 2 e 3) como condição *sine qua non* da possibilidade de entrada

equivale a dizer numa "área nuclear, inviolável e intangível da vida privada, protegida contra qualquer intromissão das autoridades e dos particulares e, por isso, subtraída a toda a ponderação de bens e interesses"[132], ainda que tais interesses se encontrem no campo e no interesse da investigação criminal.

Por outro lado, o *malware* permite a ativação do *hardware* e, consequentemente, a possibilidade de recolha de prova externa ao sistema informático, havendo claramente violação ao direito à reserva da intimidade da vida privada, o que se traduz em "devassa da vida privada[133], como também violação de outros direitos fundamentais, como o direito à palavra, quando o microfone é ativado, e o direito à imagem, quando a câmara é ligada[134].

Contudo, o *malware* pode ou não restringir o direito à inviolabilidade do domicílio. Se o *malware* for instalado remotamente e apenas se pretender a recolha de prova interna ao sistema informático, não há violação do domicílio, tendo em conta que aquele espaço permanece fisicamente inviolado, o "espaço físico da esfera privada", incluindo os sistemas informáticos que se encontrem no interior da habitação[135]. No entanto, caso o *malware* tivesse sido instalado *in loco* sub-repticiamente, passando as "barreiras físicas que delimitam a habitação", o direito à inviolabilidade do domicílio teria sido quebrado.

---

no domicílio dos cidadãos fora dos casos de mandado judicial», (*Constituição*, cit, pág. 212)". Ac.TC n.º 364/2006, processo nº 289/06. Relatora: Conselheira Maria Helena Brito.

[132] O núcleo da esfera privada é um conceito que surge da teoria das esferas de Hubmann. "Essa ideia pode ser mais bem concretizada se imaginarmos três círculos concêntricos. O externo seria o da esfera social ou pública, que está sujeita a intervenções sem altos pressupostos de justificação, e é afetado por perguntas sobre a vida social ou pública, como a profissão, ou pequenas pesquisas online sobre o que é público a respeito do investigado. O intermediário seria o da esfera privada ou do sigilo, que exige maiores pressupostos de justificação e é afetado por coleta de informações, p.ex., sobre a rotina de uma pessoa, sobre suas compras e seu círculo de amigos. E, por fim, o círculo interno seria o núcleo da esfera privada, que não comportaria qualquer intervenção". Este último é, assim, um núcleo intocável. Tratando do conteúdo essencial do direito à privacidade e é uma expressão da dignidade humana. WOLTER, Jürgen, *O inviolável e o intocável no processo penal* (…), op. cit. p. 34.

[133] Embora a jurisprudência constitucional portuguesa não tenha delimitado a proteção enquanto direito fundamental, segundo uma distinção entre "vida privada" e "intimidade da vida privada" ―por exemplo, incluindo apenas os aspetos respeitantes a um domínio mais limitado e estreitamente ligado à pessoa, ou um "núcleo central" da vida privada, tal distinção não releva para graduar a gravidade da ofensa ou para resolver o conflito com outros direitos ou interesses constitucionalmente protegidos. A proteção da vida privada na jurisprudência do Tribunal Constitucional. Relatório elaborado pelo Cons. Paulo Mota Pinto, com a colaboração da Assessora do Tribunal Constitucional, Dr.ª Raquel Reis. p. 8, disponível em https://www.tribunalconstitucional.pt/tc/conteudo/files/textos/textos0202035.pd.(consultado em 10/11/2013).

[134] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. pp. 60-61.

[135] *Idem.*

Na verdade, o direito à inviolabilidade do domicílio está intrinsecamente ligado aos conceitos de privacidade e intimidade, sendo perceptível desde logo a delimitação espacial, obstando a "uma entrada sob forma de ultrapassagem de barreiras físicas representadas pelas paredes e telhado"[136]. Este direito não se refere apenas ao ato de se entrar no espaço físico, "mas também ao abrigo dos novos meios técnicos" porque possibilitam a invasão e a devassa "do domicílio", ainda que não se observe a presença física do agente. Portanto, a violação do direito à privacidade e intimidade está para além da limitação de quatro paredes.

Como vimos, com a utilização de programas informáticos insidiosos é possível realizar a vigilância na fonte e, portanto, possibilitar o acesso ao teor desencriptado das comunicações, frustrando as medidas de autoproteção. Desta forma, poderíamos colocar a questão de se, em consequência desta intromissão,[137] é violado o direito à inviolabilidade das "telecomunicações e nos demais meios de comunicação", conforme artigo 34º, n. º4 da CRP. Na verdade, quando os interlocutores estabelecem comunicação, quer seja esta por voz, quer seja por mensagem escrita, há uma "perda de privacidade"[138], porque o processo de comunicação é mediado por operadoras de serviços de telecomunicações que, desde logo, têm acesso ao conteúdo das comunicações, o que leva a "reclamar uma tutela de comunicação durante o processo dinâmico de transmissão"[139]. Portanto, uma vez recebida a comunicação, ou todos os dados, pelo destinatário, fica afastada a possibilidade de um terceiro se poder imiscuir no conteúdo.

Não podemos esquecer que são vários os direitos fundamentais restringidos com a utilização do *malware*, dado ele ser um método oculto e haver a questão da duração que a operação que o envolve pode ter. Assim, quanto maior for o período de utilização, a monitorizar o sistema informático e a recolher dados, maior será o grau da violação dos direitos fundamentais, podendo-se aceder a um leque mais extenso de diversos dados do que em períodos curtos. Em relação ao caráter oculto, também se pode observar a intensidade da intrusão, tendo em conta que o visado desconhece a instalação sub-reptícia

[136] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 316.
[137] Mesmo nas hipóteses normais, e como o Tribunal federal alemão pertinentemente assinala, "a intromissão nas telecomunicações segundo o §. 100 a da StPO não configura apenas uma agressão, em termos de violabilidade das telecomunicações; ela representa também uma devassa da esfera privada dos respetivos intervenientes" ANDRADE, Manuel da Costa, *Sobre as Proibições* (…), op. cit. p.292
[138] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 63; ANDRADE, Manuel da Costa. *Bruscamente no Verão* (…), op. cit. p.158.
[139] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 63.

no seu sistema informático, que lhe limita os direitos de defesa. Portanto, dependendo da funcionalidade que se pretende ativar do *malware*, diversos serão os direitos fundamentais que podem ser restringidos.

5. O Princípio da Proporcionalidade

O princípio da proporcionalidade é reconhecido pelas ordens jurídicas constitucionais como importante critério normativo de valoração da atuação pública, em que se requer que a própria conduta seja racional e razoável, para que possa assim impedir uma lesão indevida dos direitos e interesses, legalmente protegidos, dos indivíduos[140].

Sucede que, no decurso da investigação criminal, pode o Estado avançar para espaços individuais constitucionalmente protegidos, mas esta restrição, no núcleo dos direitos fundamentais, é muitas vezes justificada por uma política criminal assente na trilogia de processo penal, segurança e liberdade[141]. Desta forma, a "redução de garantias processuais penais" tem vindo a ganhar "amplitude e profundidade, no quadro dos meios de obtenção de prova, em especial a abertura aos meios de maior danosidade social"[142]. Assim, justifica-se a consagração do uso do *malware,* devendo o seu regime ter especial densidade, bem como as suas funcionalidades deste meio técnico[143].

Por outro lado, a inexistência de uma "lei prevendo uma intervenção", torna "descabida a discussão se tal intervenção é possível mediante autorização judicial". A ser assim, torna-se "descabido justificar intervenções sob o *slogan* de que não há direitos absolutos ou proporcionalidade, dispensando uma lei; ainda que isso fosse correto, não cabe intervenção sem lei que a autorize"[144].

---

[140] ROCHA, Armando - Juízos de proporcionalidade – em Direito Internacional. O texto foi preparado como suporte à intervenção oral no XIII Encontro de Professores de Direito Público, realizado em Coimbra, a 24 de janeiro de 2020.

[141] VALENTE, Manuel Monteiro Guedes. Processo Penal, Segurança e Liberdade: uma provocação. *Revista Brasileira de Direito Processual Penal.* Porto Alegre, vol. I, n. 1, 2015. Segundo o autor, a "segurança tem de ser uma consequência, e nunca uma causa, da justiça processual penal e da liberdade, axiomas dotados de uma axiologia constitucional genética do ser humano. A liberdade [de todos os cidadãos] é a primeira de todas as seguranças". p. 111.

[142] *Idem*, p. 113.

[143] 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. out. — dez. de 2013. p. 233.

[144]GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal (…), op. cit. p. 1491.

Assim, na consagração do *malware* enquanto meio de prova, deve o legislador atender aos requisitos do princípio da proporcionalidade, isto é, deve fazer constar no regime jurídico, os "limites claros e específicos, em obediência àquele princípio" em que seja possível se observar a harmonia entre os critérios do princípio, a legitimação do uso do *malware* e o grau de afetação dos direitos fundamentais do individuo. De outra forma, tornar-se-ia despropositada a fundamentação de uma intervenção com recurso ao *malware* e o princípio da proporcionalidade.

Segundo as palavras de Costa Andrade[145], o catálogo de crimes deve ser completado por crimes graves, em decorrência da gravidade do meio de obtenção de prova, ou os crimes que legitimam este método. Do mesmo modo, é crucial existirem factos específicos da prática de crime para a legitimação do uso do *malware*, não subestimando que o princípio impõe que a restrição não possa ir além do estritamente necessário para um fim constitucionalmente legítimo.

De acordo com o n.º 2 do artigo 18º da Constituição, as restrições devem «*limitar-se ao necessário para salvaguardar outros direitos e interesses constitucionalmente protegidos*». É à luz deste preceito que terá lugar a aplicação dos três subprincípios em que se desdobra o princípio da proporcionalidade: idoneidade (ou adequação), necessidade (ou indispensabilidade) e justa medida (ou proporcionalidade em sentido estrito).

Desta forma, se acompanharmos a ideia do subprincípio da adequação, seria determinado *ab initio* que o uso do *malware* teria de ser adequado ao fim almejado, tendo em conta não haver restrição de outros direitos constitucionalmente consagrados. Daí, depreendemos que a legitimação do uso do *malware* em situações especificas seria um meio de prova idóneo e, de acordo com o subprincípio, conduziria a investigações mais profícuas.

Como já referido, estes novos meios de obtenção de prova, mais eficazes no combate à cibercriminalidade, são mais abrangentes e intrusivos, tornando-se necessário adequar a proporcionalidade entre os fins e os meios, ou seja, entre os direitos fundamentais individuais e o uso ilimitado dos métodos ocultos de obtenção de prova.

[145] ANDRADE, Manuel da Costa, «Métodos ocultos de investigação…», op. cit. p. 545.

Tendo em conta que, nas atividades de investigação, o uso do *malware* é reivindicado, particularmente, pelo elevado grau de eficiência, que eles podem oferecer, e considerando este meio de obtenção de prova adequado, impõe-se "fazer um juízo de respeito da sua indispensabilidade",[146] perante outros meios de obtenção de prova, existentes no nosso ordenamento, que, embora considerados aptos à obtenção do resultado pretendido, não detêm as mesmas capacidades que o *malware*.

Portanto, quer isto dizer que o uso de *malware* "revela-se essencial para apuração de crimes na atualidade"[147] se outro método não houver que seja, do ponto de "vista da respetiva lesividade menos gravoso"[148]. Daqui que, no regime jurídico, deve constar, de forma expressa, que o recurso a tal meio de obtenção de prova só se tornará viável quando não for possível encontrar, no mesmo ordenamento jurídico um outro meio suficiente ao fim visado.

Por último, o princípio da proporcionalidade, em sentido estrito, ou da razoabilidade, isto é, as medidas ou os meios legais restritivos e os fins obtidos situam-se em justa e proporcionada medida, impedindo-se, desta forma, a adoção de medidas legais, materiais e formais, restritivas e desproporcionadas, excessivas em relação aos fins obtidos[149], devendo ser feita essa ponderação entre o fim que se pretende alcançar e a lesão de direitos fundamentais, que será provocada com a intervenção. Desta forma, se os meios selecionados se mostrarem adequados e necessários, conclui-se que o meio é proporcional. Portanto, o novo regime jurídico deverá atender ao critério da gravidade do crime do catálogo e ao meio de obtenção de prova a empregar, isto é, considerar se a utilização de *malware*, no caso concreto, é adequado, indispensável e proporcional.

[146] GOUVEIA, Jorge Bacelar. *Manual de direito constitucional*, vol. II,6ª Ed., Coimbra: Almedina, 2016. pp. 825-826
[147] WEIBLEN, Fabrício Pinto. *Abertura Tecnológica* (…), op. cit. 2024. p. 47.
[148] *Idem*.
[149] VALENTE, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial*, 6ªedição Coimbra: Almedina, 2019. pp. 255-256.

CAPÍTULO III: ADMISSIBILIDADE DO *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA À LUZ DO DIREITO VIGENTE/ PREVISÃO NORMATIVA

1. O *malware* como meio de obtenção de prova interna ao sistema informático

1.1. Pesquisa de dados informáticos - Dados armazenados

A Lei 109/2009, de 15 de setembro (Lei do Cibercrime), veio introduzir novas medidas processuais em matéria de produção de prova e também ajustar outros preceitos já existentes no mesmo diploma[150], pelo que se depreende que fica, *ab inicio,* apartado o enquadramento do *malware* no artigo 174º do CPP, o qual integra o regime das buscas "tradicionais"[151]. Com efeito, ainda que se observe uma certa similitude entre o *malware* e as buscas online, entendemos não ser possível aferir a previsão daquele à luz [152]do artigo 174º do CPP, ao inverso do que sucede em outros ordenamentos jurídicos, que acolhem o *malware* no regime das buscas[153].

Portanto, se resumíssemos o *malware* a uma simples busca (*online*) "o parâmetro para aferir a sua previsão teria de ser na Lei do Cibercrime", que versa sobre os dados informáticos e "cujos cânones foram pensados para realidades intangíveis ou incorpóreas"[154] e não no artigo 174º do CPP, que consagra o regime das buscas em lugares físicos. Assim, se restringirmos o *malware* a uma simples busca informática *(online)* observamos que, de acordo com as previsões dos artigos 15º da LC e 19º do CCiber, já existe uma "atividade homónima", a pesquisa de dados informáticos, tratando-se esta de um "meio de obtenção de prova legalmente previsto"[155]. Com efeito, dispõe o artigo o 15º, n.º 1 da LC que a realização da pesquisa visa a obtenção de dados informáticos específicos e determinados "num sistema informático".

---

[150] Resultante da Convenção sobre o Cibercrime, 23 novembro 2001, e transposta para o nosso ordenamento jurídico mediante a Decisão-Quadro n.º 2005/222/JAI, do Conselho, relativa a ataques contra sistemas de informação, originando a Lei n.º 109/2009, de 15 de setembro que, por sua vez, revogou a Lei da Criminalidade Informática – Lei n.º 109/91, de 17 de agosto.

[151] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 81.

[152] *Idem*, p. 82.

[153] Nos EUA as buscas online já eram permitidas, contanto que não violassem a quarta emenda à Constituição, sendo que, inicialmente, a jurisprudência do Supreme Court considerava que só existiria violação quando a busca e/ou apreensão implicassem a entrada física em propriedade alheia.

[154] Minuta do Relatório Explicativo da CCiber, *item* 184, p. 41.

[155] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 83.

Também no n.º 5 do mesmo artigo se prevê uma forma específica de pesquisa de dados informáticos, mais concretamente quando, no decurso da pesquisa, os dados procurados se encontram noutro sistema informático, podendo então a pesquisa ser estendida a uma parte diferente do sistema pesquisado, ainda que legitimamente acessível a partir do sistema inicial, constituindo, portanto, uma "busca online que é levada a cabo remotamente"[156]. Desta forma, observa-se que, tanto a pesquisa de dados informáticos, quanto a utilização do *malware*, têm como objetivo a obtenção de dados informáticos, para além de que ambos podem ser realizados em regime presencial ou via *Internet,*[157] artigo 15º, n.º 5 do mesmo diploma.

Porém, alguns autores têm propugnado que a pesquisa também pode ser realizada remotamente, o que se traduz na possibilidade de aceder ao sistema informático via *online* [158], visto que no artigo 15º n.º 1 da LC, apenas é feita alusão aos "dados informáticos armazenados, não sendo feita referência ao modo da sua obtenção. Por outro lado, no artigo 2º al. a) da LC, é apresentado o conceito de "sistema informático", que indica que entre um ou mais dispositivos "se desenvolve a execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles", o que significa que a pesquisa de dados poderia ser efetuada em ambiente digital.[159]

Na verdade, se o preceituado no artigo 15º da LC fosse uma verdadeira busca, e a sua base de orientação fosse o regime das buscas, conforme artigo 174º do CPP, que a tem como realizada presencialmente, a pesquisa de dados informáticos também deveria acompanhar esse regime, ou seja, ser presencial. Para além de que, se observarmos o disposto no n.º 5 do mesmo artigo, apenas se referem casos que ocorram no decurso da diligência, e em que surjam "razões para crer que os dados procurados se encontrem noutro sistema informático" e que sejam "legitimamente acessíveis a partir do sistema inicial" e não a " hipóteses que se aceda remotamente e direta no sistema informático do visado"[160].

---

[156] NUNES, Duarte Alberto Rodrigues. *Os meios de obtenção de prova previstos na Lei do Cibercrime*. 2ª Edição revista e atualizada, Gestlegal, 2021. pp. 155-157.
[157] MILHEIRO, Tiago Caiado. *Comentário Judiciário do Código do Processo Penal* – Tomo II. Coimbra: Almedina, 2019. p. 845.
[158] *Idem.*
[159] MILHEIRO, Tiago Caiado. *Comentário Judiciário do Código do Processo Penal* – Tomo II. Coimbra: Almedina, 2019. p.845; Assim CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. pp. 83-84.
[160] *Idem*.

Outro ponto que aproxima a pesquisa de dados informáticos e o *malware* é o facto de ambos poderem emergir como métodos ocultos de obtenção de prova[161]. Porém, a realização da pesquisa de dados informáticos está sujeita a despacho prévio da autoridade judiciária, "com a validade de trinta dias", assim ficando garantida, ao visado, a possibilidade de ter atempado conhecimento da medida.

Todavia, a entrega do despacho prévio retira o carácter oculto à referida medida, quando, no artigo 15º, n.º 6 da LC, é feita a remissão para o regime das buscas. Assim, de acordo com o plasmado no artigo 176º, n. º1 do CPP, será entregue cópia do despacho que determinou a busca, "a quem tiver disponibilidade do lugar onde a diligência irá ser realizada, e no qual é feita a referência de que pode assistir à diligência, bem como se fazer acompanhar ou substituir por pessoa da sua confiança que se apresente sem delonga"[162]. Portanto, a cópia pode ser, por exemplo, entregue ao fornecedor de serviços, ou ao empregador. Mas se, eventualmente, não houver presente quem tenha a disponibilidade do lugar, ou "controlo sobre os dados",[163] tal formalidade pode vir a ser suprimida.

Acresce ainda, no n.º 3 da mesma norma, a possibilidade de a pesquisa ser realizada pelo OPC, sem prévia autorização da autoridade judiciária, nas seguintes situações: quando seja dado o consentimento de quem tiver a disponibilidade ou o controlo dos dados informáticos, "devendo este consentimento ficar por qualquer forma documentado"[164]. Contudo, caso o despacho, seja entregue a pessoa diversa do visado, o mesmo não terá conhecimento ou, melhor dizendo, a medida vem a ser oculta; em segundo lugar, em casos "de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou integridade de qualquer pessoa"[165], pode igualmente a pesquisa ser oculta, para o

[161] *Idem*, p. 84.
[162] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 273.
[163] Assim, CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 85.
[164] O consentimento do visado não é uma simples formalidade, ele resulta da lei e, embora não careça de forma exata, deve ser documentado, tratando-se isto de um pressuposto, ou condição de validade, da busca. Aquando do não-preenchimento dos requisitos previstos legalmente, como sendo o não consentimento do visado, geram-se proibições de prova, nos termos dos art.º 126º, n.º 3 e 118º do CPP.
[165] NUNES, Duarte Rodrigues. *Os meios de obtenção* (…), op. cit. pp. 216-217; no mesmo sentido, CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 85; JESUS, Francisco Marcolino de. *Os Meios de Obtenção da Prova em Processo Penal*-2. a Edição. Leya, 2015. p. 169.

visado. Nestes sentidos, a pesquisa nem sempre é conhecida do visado.[166] Portanto, à semelhança de outros meios ocultos da obtenção de prova, a pesquisa de dados informáticos é também um meio de obtenção de prova muito invasivo, como a utilização do *malware*, sendo este mais um aspeto que os aproxima.

Se, por um lado, são visíveis alguns aspetos que aproximam as buscas informáticas do uso de *malware*, por outro, eles também se distanciam, noutros pontos, pois a pesquisa de dados informáticos incide sobre dados específicos e determinados, ao passo que o *malware* é um programa informático instalado clandestinamente que acede, não só aos dados armazenados no sistema, como também aqueles que não estão ali armazenados e ainda aos produzidos em tempo real.

Ainda há que considerar que, de acordo com o plasmado no artigo 15º, n.º 5 da LC, é permitida a extensão da pesquisa de dados informáticos "quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado", enquanto o uso do *malware* possibilita o acesso direto ao sistema informático pretendido[167].

Desta forma, entendemos que a utilização do *malware* não é compatível com o regime das pesquisas, conforme previstas no artigo 15º da LC.

1.2. A apreensão de dados informáticos

Na sequência da pesquisa, eventualmente segue-se a apreensão de dados informáticos, conforme o disposto no artigo 16º da LC, que consiste em a AJ colher, para o processo, dados informáticos, (de acordo com o conceito constante do artigo 2º , al. b, da LC, que inclui os documentos informáticos e os chamados meta-dados) que se encontrem num sistema informático ou em suporte autónomo, na decorrência da

[166] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p .86; REAL, Rui Miguel dos Santos, Apreensão, exames ou perícias e utilização processual de meios de prova existentes em material informático ebook cej p. 150.
[167] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 87.

diligência, isto é, no decurso da pesquisa, e que sejam determinantes à descoberta da verdade material e/ou, ainda, que sirvam de prova.[168]

O nosso legislador faz a distinção entre apreensão de dados informáticos — artigo 16º da LC — e apreensão de correio eletrónico e registo de comunicações de natureza semelhante — artigo 17º da LC. Contudo, no artigo 19º da CCiber não é feita qualquer alusão a esta distinção.

Como atrás referido, a apreensão de dados informáticos comporta uma função de complementaridade à pesquisa de dados, como sucede com o *malware* que, uma vez instalado, tem igualmente como função o envio dos dados informáticos apreendidos à AJ, mas tal não é o bastante para que seja considerado um método legítimo[169], pelo que essa sua descrita função não se confunde com a apreensão de dados informáticos.

Ademais, a apreensão de dados informáticos surge na sequência de uma pesquisa, um acesso legitimo, o que não acontece com o *malware*, assim como a apreensão pode nem sequer se revestir duma natureza oculta, e somente se restringir a obter dados armazenados. Portanto, entendemos que o alcance da devassa é menor do que a do uso de *malware.*

1.3. Dados produzidos em tempo real

Como mencionado, o *malware* faculta a obtenção de dados em tempo real, assim como permite o acesso a um conjunto elevado de informações contidas num sistema informático. E, ao permitir a vigilância na fonte das comunicações, poderíamos enquadrá-lo no âmbito do artigo 18º da LC, que prevê a interceção de comunicações.

Contudo esta possibilidade fica apartada, tendo em conta alguns aspetos. Primeiramente, por a vigilância na fonte não se confundir com a interceção de comunicações. Depois, porque o artigo 18º da LC, ao invés do caso do *malware*, exclui a recolha por via remota e oculta de dados armazenados e não armazenados no sistema

[168] NUNES, Duarte Rodrigues. *Os meios de obtenção* (…), op. cit. p .260.
[169] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 88.

informático, limitando o acesso a dados de tráfego, ou de conteúdos referentes a comunicações.

Por último, como sabemos, o *malware* é um meio de obtenção de prova muito invasivo, uma vez que possibilita o acompanhamento de toda a atividade praticada pelo suspeito, no sistema informático, em tempo real, sem que, para tal, seja necessária a ocorrência de qualquer comunicação.

Por outras palavras o *malware* tem uma maior abrangência do que uma interceção, pois permite a recolha de diversas informações e dados contidos no sistema informático, esteja este em processamento ou aqueles armazenados, para além de possibilitar a captação de toda a atividade externa ao sistema informático, enquanto que a interceção é limitada ao tipo de dados que visa intercetar, logo a subsunção do *malware* no regime do artigo 18º da LC seria ostensivamente redutor.

Por fim, cabe sublinhar que o *malware* também não se confunde com a interceção de comunicações, mesmo que se possa traduzir numa ingerência das autoridades nas interceções. Neste sentido, nos termos do artigo 34º, n. º4 da CRP e do artigo 126º, n.º 3 do CPP, um meio da obtenção de prova que resulte em intromissão ou ingerência das autoridades públicas nas telecomunicações e nos demais meios de obtenção de comunicação, só é admissível nos casos previstos na lei, pelo que legitimar o uso do *malware*, ao abrigo do artigo 18º da LC. º, traduzir-se-ia numa inconstitucionalidade material, por violação do artigo 18º, n.º 2 e do 34º, n.º 4 da CRP.[170]

2. Dados Armazenados e dados produzidos em tempo real

2.1. Ações Encobertas em Ambiente Digital

Do anteriormente considerado, ficou apartada a possibilidade de os artigos 15º a 18º da LC consubstanciarem alguma base legal para o uso do *malware* na investigação criminal. Pretendemos agora analisar o regime das ações encobertas em ambiente digital, previstas no artigo19º do mesmo diploma.

[170] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 90.

É sabido que o "crime tende a seguir a oportunidade" [171] e a *internet* é fértil em propiciar oportunidades, sendo visível o deslocamento de uma grande parte da vida em sociedade para o ciberespaço e, consequentemente, também o aumento da cibercriminalidade, o que trouxe novos desafios, em matéria de recolha de prova, e criou dificuldades à investigação. Na verdade, a utilização do *malware* na investigação criminal é cada vez mais frequente, em razão do elevado potencial por si demonstrado, na recolha de prova, tendo em conta que permite o acesso remoto a todas as informações armazenadas no sistema informático do suspeito e, ainda, aos dados produzidos em tempo real.

O ordenamento jurídico português já consagra um meio de obtenção de prova de características semelhantes ao *malware*, que são as denominadas "ações encobertas em ambiente digital"[172], e que encontram base legal no artigo 19º da LC.

Assim, institui o artigo 1º n.º 2, da Lei 101/2001, de 25 de agosto, em que se consideram "ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal, ou por terceiro atuando sob o controlo da Polícia Judiciária, para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade", cabendo assim aqui a previsão legal da figura do agente encoberto[173]. Todavia, no que diz respeito à figura do agente encoberto em ambiente digital[174], inexiste

[171] PELLUCCI, Frederico. A atuação dos agentes encobertos e infiltrados nos canais, abertos e fechados, de comunicação, em ambiente informático-digital. In: Novos desafios da prova penal / coord. Paulo de Sousa Mendes, Rui Soares Pereira. - Coimbra: Almedina, 2020. p. 237.

[172] À semelhança das apreensões de correio eletrónico e do registo de comunicação, não consta na CCiber qualquer norma com previsão específica das ações encobertas, em ambiente informático digital, tratando-se isso de uma criação do nosso legislador, ao abrigo da sua liberdade de conformação.
Já no ordenamento jurídico alemão, inexistem normas referentes às ações encobertas online, e aplicam-se os §§ 110 a ,110 c StPO, que são as disposições destinadas às ações encobertas clássicas. NUNES, Duarte Rodrigues. *Os meios de obtenção* (…), op. cit. p. 428.
Em Espanha, a figura do agente encoberto informático encontra-se prevista no artigo 282.º n.ºs 6 e 7 bis, da LEC, através da LO 13/2015, aplicando-se as mesmas disposições e condições que para o agente encoberto tradicional. Em Portugal, as ações encobertas tradicionais encontram-se previstas na lei n.º 101/2001, 25 de agosto.

[173] Lei 101/2001 artigo 1.º n.2: o agente encoberto é o funcionário de investigação criminal ou um terceiro.

[174] Para Guedes Valente, a figura do agente infiltrado pode ser física ou digital, e encontra-se regulada no artigo n.º 19 da LC, sendo este um meio de obtenção de prova oculto, intrusivo e lesivo dos direitos fundamentais. O agente infiltrado digital "tem como função ganhar a confiança dos demais membros do grupo restrito ou fechado", podendo o acesso "ser livre, mas o contato e a assimilação de informações, restrita" e, com este método, procura-se "obter informações, meios de prova, ou provas, destinados a prevenir e a reprimir crimes". VALENTE, Manuel Monteiro Guedes. *Teoria Geral* (…), op. cit. pp. 616-617.

qualquer previsão expressa na lei, ao invés do que sucede noutros ordenamentos jurídicos[175].

Este regime das ações encobertas tem suscitado algumas controvérsias doutrinárias, pela remissão do artigo 19º n.º 1 da LC para o RJAE (Lei n.º 101/2001, de 25), ou seja, ao se aplicar, em parte, o regime geral das ações encobertas em ambiente físico ao ambiente digital.

Como já referido, as ações encobertas são levadas a cabo por funcionários ou por terceiros, que convocam a figura dos "homens de confiança" (*Vertrauensmann*) [176], sendo permitida a ocultação da sua identidade, e que atuam sob o controlo da AJ, no combate aos crimes nessa lei previstos.

Contudo, é importante fazer ressaltar que, dentro da categoria dos "homens de confiança"[177], de facto somente são aceitáveis os agentes encobertos ou infiltrados[178], não sendo admissível a figura do agente provocador, que é definido como membro da autoridade policial ou civil, comandado pela polícia, que induz alguém a delinquir, de forma a propiciar a recolha de prova da ocorrência do facto ilícito[179].

Segundo Germano Marques da Silva, "a provocação não é apenas informativa, mas sobretudo formativa, não revela o crime e o criminoso, mas cria o próprio crime e o criminoso e, por isso, é contrária à própria finalidade da investigação criminal, uma vez que gera o seu próprio objeto"[180]. O agente provocador incita o suspeito ao cometimento

[175] Em Espanha encontra-se regulado por via dos números 6 e 7 do artigo 282 da LECrim, com a entrada em vigor da LO 13 /2015, que consagra a figura do agente encoberto informático, deixando claro que se lhe aplicam as condições fixadas para o agente encoberto tradicional.

[176] Os homens de confiança, "*Vertrauensmann*", aqueles que colaboram com as instâncias formais da perseguição penal tendo como contrapartida a promessa da confidencialidade da sua identidade, ANDRADE, Manuel da Costa. *Sobre as proibições de prova em processo penal*. 2.ª edição Gestlegal, 2022, p. 228. Nesta categoria se incluem "particulares pertencentes ou não ao submundo da criminalidade", bem como agentes da investigação criminal que, de forma disfarçada, se introduzem naquele submundo, ou com ele entram em contato, e que se limitam a recolher de informações, e que vão ao ponto de provocar, eles próprios, a prática do crime. SOUSA, Susana Aires de. "*Agent provocateur* e meios enganosos de prova. Algumas reflexões." *Liber Discipulorum para Jorge de Figueiredo Dias*, 2003. p. 1221.

[177] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. pp. 300-301.

[178] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 92.

[179] SOUSA, Susana Aires de. *"Agent provocateur* (…), op. cit. p. 1222.

[180] SILVA, Germano Marques da. "Bufos infiltrados (…)". p. 29.

de factos ilícitos "agindo, por exemplo, como comprador recetor ou fornecedor de bens e serviços ou serviços ilícitos"[181] .

Assim, no decurso de uma investigação em ambiente digital, poder-se-ia fornecer "material ilícito infetado com *malware"*[182] ou criar *hyperlinks* (método oculto próximo das ações encobertas), que permitem aceder a conteúdos[183], bastando um mero acesso ao *link*, para que o IP seja recolhido, dado conhecimento à AJ ou aos OPC do endereço da ligação a partir da qual partiu a comunicação, e iniciada a investigação. Este tipo de usos convidar-nos-ia a entrar num plano de "atividades provocadoras"[184] em ambiente digital, através do uso do *malware*.

Por outro lado, também se observa que, tanto as ações encobertas como o *malware*, permitem a recolha de dados produzidos em tempo real, bem como de dados armazenados, e que ambos são métodos ocultos. Sucede que, de entre os métodos ocultos de investigação criminal, no nosso ordenamento, o agente encoberto é aquele que mais controvérsia tem suscitado na doutrina[185], por se assumir como figura jurídica que, ao abrigo da lei, omite dolosamente a "identidade e qualidade",[186] com a finalidade de captar o outro no cometimento de um delito, o que levanta questões de natureza jurídica, no plano da lealdade processual, em que o Estado é dotado de um poder de superioridade, o *ius puniendi*, mas que se quer de "mãos limpas".[187] Por seu turno, também o *malware* é

---

[181] SOUSA, Susana Aires de. *"Agent provocateur* (…), op. cit. p. 1223.

[182] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 93.

[183] *Hiperlinks sting operation* nos EUA; sites coruja, *(sitti civetta)* na Italia. Os *hiperlinks* surgem como novas vias para detetar práticas de ilícitos no âmbito da pornografia infantil, consistindo na criação e publicitação, por parte das autoridades responsáveis pela investigação criminal, e que darão o acesso imediato a conteúdos de natureza pornográfica infantil. RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 309.

[184] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 93.

[185] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 286.

[186] Segundo David Silva Ramalho, a ocultação da qualidade identidade do agente é um elemento particularmente grave. Pois não se refere apenas a mera revelação da entidade num determinado contexto, mas sim de uma conduta ativa do encobrimento da identificação do agente (em que numa outra situação o agente não fardado diria que se identificar onde quer que fosse) e caso necessário o recurso à mentira, conduta oposta às regras vigentes na vida em sociedade. O agente para além da ocultação da identidade, infiltra-se no grupo dos criminosos e sequentemente tenta ganhar a confiança dos suspeitos, que por último, vem permitir ao agente a recolha de material probatório da prática ato ilícito, a qual conduzirá á responsabilização criminal do mesmo. Acontece que em ambiente digital é vulgar a criação de perfis falsos e a criação de um *usename* de todos os intervenientes. RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. pp. 292-293.

[187] SOUSA, Susana Aires de. *"Agent provocateur"* (…), op.cit. p.1212, RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 287.

instalado sub-repticiamente no sistema informático do visado, de forma oculta, fazendo-se passar por *software* de atualização, ou outra qualquer inocuidade.

Apesar de as ações encobertas em ambiente digital e o *malware* se aproximarem nos aspetos já referidos, eles também se distanciam. Assim, as primeiras são levadas a cabo por agentes, funcionários de investigação criminal ou terceiros, pretendendo-se ganhar a confiança dos demais membros de um grupo restrito ou fechado [188], enquanto o *malware* é um programa simples ou autorreplicativo que se instala num sistema informático, sem o consentimento do visado, não existindo qualquer interação humana de aparência normal, muito menos a pretensão de se estabelecer uma relação de confiança, mas antes uma recolha, previamente programada e automática de *motu proprio* de material probatório.

Questão central é a de se saber se é permitido o uso do *malware,* no âmbito da investigação criminal, cuja resposta afirmativa tem sido sustentada por alguma doutrina. Segundo a previsão do artigo 19º, 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 interceção de comunicações". O legislador não foi claro quanto ao significado de "meios e dispositivos informáticos", o que suscita ao intérprete uma dificuldade de densificação normativa, quanto a tal conceito.

No entendimento de David Silva Ramalho, a expressão "meios e dispositivos informáticos", suscita questões de natureza teleológica, pois estes meios não se subsumem aos outros meios de obtenção de prova previstos no CPP, o que levou o legislador a introduzir um novo preceito, com a finalidade de legitimar o seu recurso. A norma nasce da necessidade de colmatar as insuficiências das caracterizações de outros meios de obtenção de prova já existentes. Caso contrário, ela se tornaria redundante e supérflua, permitindo tão somente aos agentes encobertos acederem aos meios já previstos no nosso ordenamento[189]. Assim, segundo o autor, o regime de admissibilidade do uso do *malware* nas ações encobertas adviria do artigo 19º, n.º 2 da LC, somente seria

[188] VALENTE, Manuel Monteiro Guedes. *Teoria Geral do Direito Policial*, 6ª edição Coimbra: Almedina, 2019. op. cit. p. 617.
[189] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. pp. 344-345.

admissível para fins de prevenção e repressão criminal, em casos devidamente identificados e tendo em conta a gravidade do crime[190].

Acresce que a remissão do n.º 2 da LC, para o regime da interceção de comunicações do CPP, "naquilo que for aplicável", leva a que, segundo Benjamim Rodrigues, "as ações encobertas, ao nível da Lei do Cibercrime, implicarão a necessidade do respeito pelas regras do regime das escutas telefónicas, sempre que elas implicarem o recurso a meios e dispositivos informáticos ligados às tecnologias da informação e comunicação, e isso ocorrer por meio das redes eletrónicas publicamente acessíveis"[191].

Quanto a esta questão, no nosso entendimento, dúvidas não restam: as ações encobertas são o meio oculto de obtenção de prova que se reveste de carácter excecional e, portanto, só deve ser usado em último recurso. Assim como a ocultação da identificação e o engano que acompanham *ab inicio* a atuação do agente infiltrado, essas ações comportam "graves repercussões em direitos fundamentais", ainda que se pretendam tão-somente informações de interesse à investigação[192]. Também não acompanhamos a posição daquela corrente doutrinária que defende que o art. 19º, n.º 2 da LC permite o acesso a "outros meios", para além dos já previstos no nosso ordenamento.

Vejamos: a expressão "meios e dispositivos informáticos" surge como manifestação ou aceção indeterminada, o que convoca o princípio da determinabilidade dos atos normativos[193], colocando-nos num campo de imprecisão quanto à sua aplicação com a segurança e a certeza exigidas. Pelo que entendemos que o recurso ao *malware* não se encontra legitimado, pois trata-se de um meio que facilmente lesa direitos, liberdades e garantias, quer do suspeito quer de terceiros, limites constitucionalmente impostos, como o direito à reserva da intimidade da vida privada, da inviolabilidade do domicílio e da correspondência ou das telecomunicações. Assim, cremos que o *malware* necessita de regulamentação autónoma, densa, expressa e determinada, assim se conseguindo essa legitimação.

---

[190] *Idem*, p. 347.

[191] RODRIGUES, Benjamim Silva, *Da prova penal*, Tomo II. Bruscamente...a(s) face(s) oculta(s) dos Métodos Ocultos de Investigação Criminal, 1.ª ed., Rei dos Livros, 2010. p. 130.

[192] PELLUCI, Frederico. A atuação dos agentes encobertos e infiltrados nos canais abertos e fechados de comunicação em ambiente informático-digital. In: Novos desafios da prova penal / coord. Paulo de Sousa Mendes, Rui Soares Pereira. - Coimbra: Almedina, 2020. p. 249.

[193] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p.92.

3. Meios de obtenção da prova externa ao sistema informático

Como referido, o uso do *malware* permite a recolha de uma multiplicidade de informações, de dados contidos nos sistemas informáticos, "estejam eles em processamento ou simplesmente armazenados", para além de "possibilitar a captação de sinais audiovisuais emitidos no raio de alcance dos seus componentes"[194]. Além disso, a infiltração possibilita a "recolha de prova externa ao sistema informático"[195], com a ativação do *hardware*, isto é, ativação da *webcam* e o microfone, possibilitando a captura de som e imagem[196].

No nosso ordenamento jurídico, encontramos já meios de obtenção de prova que permitem recolha de prova externa a um sistema informático, caso do registo de voz e imagem, no artigo n.º 6 das medidas de combate à criminalidade organizada, Lei nº 5/2002, de 11 de janeiro, e artigo 189º, n.º 1 *in fine*, do CPP, "a interceção de comunicações entre presentes", mas ambos não se confundem.

Relativamente aos pressupostos de admissibilidade destes meios ocultos de obtenção de prova, no caso da "interceção de comunicações entre presentes", elas somente podem ser autorizadas durante o inquérito, e se houver razões para crer que a diligência é indispensável à descoberta da verdade que, de outra forma, seria impossível, ou muito difícil, de obter, conforme dispõe o artigo 187º do CPP. No que respeita ao meio de recolha de voz e imagem, os requisitos são menos exigentes, sendo admissível a recolha quando necessária para a investigação de crimes do catálogo, por qualquer meio, sem o consentimento do visado, nos termos do artigo 6.º da Lei n.º 5/2002, captando apenas voz e imagem em conversações ou outras comunicações do suspeito, pelo que o seu alcance quanto à recolha de material probatório é superior ao das interceções de comunicações entre presentes, pois "pressupõe a existência de um interlocutor ―conversa ou comunicação"[197].

---

[194] RIBEIRO, Gustavo A. M.; Cordeiro, Pedro Ivo R. V.; Fumach, Débora M. O *malware* como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. *Revista Brasileira de Direito Processual Penal*, vol. 8, n. 3, p. 1463-1500, set./dez. 2022. p. 1465.
[195] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 97.
[196] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 350.
[197] *Idem*, p. 98.

Na verdade, de acordo com o disposto no artigo 189º, n. º1 do CPP, apenas se contempla a "interceção de comunicações entre presentes", e o artigo 6º, n. º1 determina o "registo de voz e imagem, por qualquer meio", sendo ambos meios ocultos de obtenção de prova, o que nos poderia levar a crer que o uso do *malware* se encontraria legitimado. Não obstante, considerámos que o *malware* não se enquadra nos preceitos em análise pois, conforme se disse, este meio de recolha de prova abrange não só dados armazenados, dados em tempo real, como também permite "a captação de toda a atividade , através da *webcam* e dos microfones", transformando-se num mecanismo invisível de vigilância do suspeito no interior da sua habitação, no seu domicílio, o que se tornaria "numa espécie de grande devassa digital"[198].

Assim, visto que o uso do *malware* possibilita a ativação da *webcam* ou dos microfones na habitação do visado, fica *ab inicio* apartada a hipótese de os preceitos legais em análise consubstanciarem uma base legal para o uso do *malware*, tanto pelo artigo 6, n.º 1, como pelo artigo 189º, n.º 1 do CPP, na "interceção de comunicações entre presentes", sendo estas apenas permitidas durante o inquérito, por despacho fundamentado do juiz de instrução, e em situações muito excecionais[199].

Desta feita, nem o uso do *malware* se enquadra em nenhuma das normas apreciadas, nem ele pode ser utilizado para ativar o *hardware* do sistema informático infetado, de modo permitir a captação de som imagem[200]. Assim, imaginando o uso do *malware* num determinado caso concreto, e tendo em conta que se trata de um meio oculto de prova particularmente intrusivo e insidioso, consideramos que as suas características não se coadunam com os requisitos menos exigentes do artigo 6º da Lei n.º 5/2002, ou seja, sempre que "necessário para a investigação de crimes referidos" no catálogo, é permitido "o registo de voz e de imagem, por qualquer meio". Para além de que o objetivo do *malware*, enquanto meio de recolha de prova digital, é o de colher dados informáticos armazenados ou dados em tempo real, e não o de funcionar de modo idêntico ao dos referidos preceitos.

---

[198] RAMALHO, David Silva, *Métodos ocultos* (…), op.cit. p. 349; PINHEIRO, Alexandre Sousa - *Privacy e protecção de dados pessoais*: a construção dogmática do direito à identidade informacional. Lisboa: AAFDL- Associação Académica da Faculdade de Direito de Lisboa, 2015. pp. 489-490.

[199] MILHEIRO, Tiago Caiado, comentário ao artigo 189; CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 99.

[200] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 350.

No nosso entender, o uso do *malware* somente é admissível se se verificar uma suspeita fundada[201] da prática de um crime do catálogo, e que esse uso é necessário para e indispensável a descoberta da verdade material, que, por isso, seria impossível de obter doutra forma. Não obstante, apesar destes elementos já se encontrarem previstos no artigo 189º, n. º1 do CPP (com remissão expressa para o artigo 187º do mesmo diploma), continuamos a crer que o recurso ao *malware* ainda não se encontra legitimado[202].

4. O *Malware* como Método Atípico

Retomando palavras de Germano Marques da Silva, os meios de obtenção de prova são "instrumentos de que se servem as autoridades judiciárias para investigar e recolher meios de prova; não são instrumentos de demonstração do *thema probandi*, não são meios de prova, são instrumentos para recolher, no processo, essoutros instrumentos". Os meios de obtenção de prova distinguem-se dos meios de prova, sendo estes últimos "os elementos de que o julgador se pode servir para formar a sua convicção sobre um facto"[203].

No nosso ordenamento jurídico[204], a atipicidade dos meios de obtenção de prova tem previsão legal no artigo 125º do CPP que prescreve, sob a epígrafe a "legalidade da prova", que são admissíveis todas as provas que não forem proibidas por lei. Quer isto dizer que o conjunto dos meios de prova e, naturalmente, dos meios de obtenção de prova "admitidos em processo penal, não se encontra limitado ao catálogo legal"[205], incluindo também meios de prova e meios de obtenção de "prova inominados ou atípicos" e, portanto, vigora a regra da não taxatividade[206].

---

[201] CAMPOS, Juliana Filipa Sousa, *O Malware* (…), op. cit. p. 100.
[202] Assim, CAMPOS, Juliana Filipa Sousa, *O Malware* (…), op. cit. p. 100.
[203] SILVA, Germano Marques da. *Curso de Processo Penal II,* 5.ª Ed., Lisboa: Verbo, 2011. p. 280.
[204] Grande parte dos ordenamentos jurídicos da *civil law* adota a regra da não taxatividade, atipicidade e liberdade de produção de provas. Nos países da tradição do *common law*, a regra geral é a admissibilidade de todos os meios de investigação, independentemente da previsão legal. WEIBLEN, Fabrício Pinto. *Abertura Tecnológica* (…), op. cit. 2024. p. 47.
[205] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 213.
[206] o CPP consagra a regra de não taxatividade dos meios de prova. Os meios de prova atípicos estão subordinados aos limites constitucionais e legais de admissibilidade da prova resultante do artigo 126º do CPP.

No entanto, não poderá decorrer do artigo em causa o entendimento de legitimar o recurso a qualquer meio de obtenção de prova, "descurando os limites constitucionais e legais que subjazem à aquisição probatória",[207] nem a concordância prática das finalidades do processo penal de um Estado de direito democrático.

Numa leitura superficial, conjugando o artigo 125º com o 126º do CPP, sob a epígrafe "Métodos proibidos de prova", que dispõe que "são nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral das pessoas", seriam admitidos quaisquer meios de prova e meios de obtenção de prova, desde que não legalmente proibidos.

Em processo penal vigora o princípio da legalidade e "não da atipicidade da prova, de onde decorre que a prova deve ser feita, não apenas nas margens da não proibição, mas sim nos termos da lei, exceto quando esta se revele insuficiente e não haja obstáculo ao recurso a meios de prova ou de obtenção de prova atípicos" [208].

Como já afirmado, o *malware* não encontra previsão legal no nosso ordenamento. Por outro lado, não pode este meio de obtenção de prova ser legitimado ao abrigo de uma qualquer disposição referente aos meios de prova consagrados na lei processual penal. Assim, quando o meio de obtenção de prova "implicar um elevado grau de intrusão na privacidade do suspeito, com potencial aditivo de perigo inerente ao ataque dos direitos fundamentais" ele deve ser previsto por uma lei expressa, salvo consentimento expresso e informado do visado"[209], pelo que se impõe a sua legitimação da atividade correspondente a precedência de lei formal habilitante,[210]ou decreto-lei autorizado pela Assembleia da República, conforme dispõe os artigos 18º, n.º 2 e 3, e 165º, alínea b) da CRP.

Por tudo o exposto, o *malware* não pode ser acolhido como meio de obtenção de prova atípico, uma vez que o seu uso pode restringir um leque de direitos fundamentais, não respeitando os limites constitucionais impostos no artigo 34º n.º 2 e 4 e no artigo 32 º n.º 8, ambos da CRP, que determinam a nulidade das provas obtidas sob tortura ou coação, obtidas

[207] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 105.
[208] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 214.
[209] *Comentário do código de processo penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos* / org. ALBUQUERQUE. Paulo Pinto de - 5ª ed. atualizada. - Lisboa : Universidade Católica Editora, 2023, pp. 486-487.
[210] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 216.

com ofensa da integridade pessoal, da reserva da intimidade da vida privada, da inviolabilidade do domicílio e da correspondência ou das telecomunicações nem os limites legais, em conformidade com o disposto na Constituição, que resultam do artigo 126.º do CPP.

CAPÍTULO IV: O USO DO *MALWARE* NOUTROS ORDENAMENTOS JURÍDICOS E EM PORTUGAL

1. Abordagem comparatística do *malware* noutros ordenamentos jurídicos

O potencial de recolha de prova demostrado pelo uso do *malware* levou a que alguns ordenamentos jurídicos viessem a legitimar o recurso a esse meio. Na verdade, o *malware* tem uma capacidade de resposta às técnicas anti-forenses dificilmente igualável por qualquer outro instrumento jurídico já existente, pelo que este meio já vinha sendo empregue nas investigações criminais, "sem qualquer base"[211].

Assim, no que se segue, faremos uma breve análise às alterações legislativas que visaram a introdução do *malware* nos ordenamentos jurídicos norte-americano, alemão e espanhol.

2. Experiência norte americana

Iniciamos pela experiência americana, que, para além de pioneira, tem sido muito turbulenta, nas últimas décadas, desde logo, pautada várias e repetidas divulgações não autorizadas de uso secreto de vários tipos de *malware*, por parte das autoridades.

O primeiro caso sobre o uso de *keyloggers* remota a janeiro de 1999, no âmbito de uma investigação criminal levada a cabo pelo FBI ao cidadão Nicodemo S. Scarfo. Era um individuo conhecido, "membro de uma organização mafiosa, suspeito do cometimento de infrações criminais relacionadas com a gestão de um negócio de jogo ilegal" e, no decurso da investigação, descobriu-se que guardava no seu computador "ficheiros cifrados" que se poderiam revestir de alto valor probatório[212]. Para poder

[211] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 105.
[212] United States v. Scarfo, U.S. District Court for the District of New Jersey - 180 F. Supp. 2d 572 (D.N.J. 2001) December 26, 2001. Em maior detalhe no acórdão disponível em: https://law.justia.com/cases/federal/district-courts/FSupp2/180/572/2475159/ (consultado em 20/10/2023); RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 311-312.

decifrar os conteúdos encriptados, o FBI solicitou um mandado judicial, para introduzir um *keylogger* no computador do suspeito, de modo a obter a palavra-passe.

Na altura, a instalação de *keyllogers* não era tarefa fácil, pois exigia a presença física para se proceder à instalação, atuação direta nos computadores dos suspeitos. Entretanto, com o aumento da criminalidade internacional, sobretudo depois do ataque às Torres Gémeas, o desenvolvimento desta área levou a que estes procedimentos viessem a ser praticados remotamente.

É neste contexto que surge o *Magic Lantern*, um *keylogger* concebido para ser instalado de forma sub-reptícia e remota no sistema informático do visado, quando se trate de suspeitos relacionados com atividades perigosas, em particular de natureza terrorista[213].

O *Magic Latern* veio a ser substituído pelo *Computer and Internet Protocol Adress Verifier, em* 2007, ou CIPAV, um *malware* também criado pelo FBI que, de entre outras funcionalidades, permitia a recolha do endereço IP e/ou MAC[214]do suspeito, bem como a localização e a lista de programas em funcionamento num dado momento, como websites visitados ou contas abertas. Este *software* foi utilizado em vários casos, porém os seus resultados somente publicados em 2007, com o processo Timberlinebombinfo.[215]

A publicação destes documentos permitiu tirar duas conclusões: "a primeira foi de que este programa era abundantemente utilizado, por entidades governamentais e não pelo FBI"; a segunda, de que não existia concordância quanto aos requisitos de admissibilidade: Um dos polos albergava os defensores da desnecessidade de qualquer procedimento legal para a sua utilização, e o outro acolhia os partidários de que a sua utilização dependeria de autorização judicial"[216]. Não se conseguindo harmonização, o FBI solicitou um parecer jurídico quanto aos requisitos do quadro jurídico ao uso destes *softwares*, obtendo, como resposta, "a necessidade de um pedido de mandato judicial com

[213]RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 325.
[214] "Os endereços MAC (*Media Access Control*) [...] fazem parte da ligação de dados, e podem ser utilizados para identificar um computador específico numa rede. - Casey, 2011: 624. RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 206.
[215] JULIEN LAUSSON, « Le mouchard de la police allemande vise aussi Skype, Gmail, Facebook … », Numerama, 10-10-2012, disponível em https://www.numerama.com/politique/23989-le-mouchard-de-la-police-allemande-vise-aussi-skype-gmail-facebook.html (consultado em 20/10/2023).
[216] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 326.

duas vertentes: por um lado, autorizar a realização da busca, assim legitimando a autorização da intrusão no computador e, por outro lado, autorizar o registo das comunicações".

Contudo, o recurso ao *malware* no âmbito das investigações criminais não cessou. Com efeito, em 2012, surge a Operação Torpedo, na qual não foi concedida autorização judicial, no decurso de uma investigação, para o uso do *malware*. Tratava-se de duas condutas criminalmente relevantes: "o acesso ilegítimo a uma conta de e-mail de um cidadão norte-americano e a respetiva utilização para acesso à sua conta bancária; e a criação de uma conta de e-mail praticamente idêntica para, subsequentemente, se dar uma ordem de transferência, da conta bancária do mesmo cidadão para um banco estrangeiro"[217].

O pedido da referida autorização foi feito ao abrigo do regime aplicável às buscas e apreensões, do artigo 41 das *Federal Rules of Criminal Procedure* (FRCP), e assentou em que a instalação de *malware* se subsumia ao conceito de busca, e a extração e o envio de informações remotamente, ao conceito de apreensão. O novo tipo de *malware* veio possibilitar a recolha de registos de atividade na Internet e de registos do utilizador, controlar remotamente o sistema informático do visado, gerar coordenadas de latitude e longitude, recorrer à webcam, permitindo a identificação do suspeito e do local em que se encontra[218].

Contudo, as buscas online já eram permitidas, contanto que não violassem a quarta emenda à Constituição, sendo que, inicialmente, a jurisprudência do Supreme Court considerava que só existiria violação quando a busca e/ou apreensão implicassem a entrada física em propriedade alheia [219]. Mais tarde, o mesmo Tribunal (na sentença *Katz v. United States*[220]) abandonou essa posição, e ampliou o âmbito de proteção da Quarta Emenda, considerando que a referida tutela não se limitava à apreensão de bens corpóreos, mas passava a incluir as interceções e gravações de conversas e comunicações,

[217] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 327.
[218] *Idem*, p. 328.
[219] Olmstead v. United States (1928) e Goldman v. United States (1942) do Supreme Court of the United States, disponível em https://supreme.justia.com/cases/federal/us/277/438/ (consultado em 29/10/2023); NUNES, Duarte Rodrigues. *Os meios de obtenção* (…), op. cit. p. 486.
[220] Katz v. United States do Supreme Court of the United States (1967), disponível em https://constitutioncenter.org/blog/katz-v-united-states-the-fourth-amendment-adapts-to-new-technology?gad_source=1&gclid=CjwKCAjwl4yyBhAgEiwADSEjeGaH_1T9pYS8aB2tPY3DHlPor1VN4YlXQ_tP93a-on7E99qasoGSyhoCmd0QAvD_BwE (consultado em 29/10/2023).

e não abrangia apenas espaços, mas também pessoas, contanto que "uma pessoa tenha uma expectativa razoável de privacidade, a menos que certas exceções se apliquem", pelo que a violação da Quarta Emenda passava a não depender da entrada física das autoridades em propriedade privada, mas da existência de uma expectativa razoável de privacidade.

Quanto ao pedido concreto, o Tribunal conclui pelo indeferimento, afastando desde logo a sua competência territorial para emitir qualquer tipo de busca, referindo ainda que os dados não se encontram numa nuvem, mas sim armazenados em sistemas informáticos concretos, pelo que estariam sujeitos às regras sobre onde se encontravam.

Analisando o pedido à luz da quarta adenda à Constituição, o Tribunal constatou que este tipo de *malware* não garantia que somente o mínimo necessário de dados seria recolhido, nem tão-pouco garantia que apenas os visados seriam alvos da medida, tendo em conta que poderão os agentes do crime ter utilizado o IP de um terceiro, estando então o seu sistema informático localizado, por exemplo, numa biblioteca pública, num café, ou num local de trabalho acessível a várias pessoas. Por outro lado, a possibilidade de envio de *malware* por e-mail para o visado não garante que não haja outras pessoas, com acesso à mesma conta, que possam inadvertidamente instalar o *malware* no seu próprio sistema informático[221].

O Tribunal considerou também que a ativação da câmara do sistema informático é componente de uma atividade de videovigilância, pelo que devem ser observáveis os requisitos adicionais de indispensabilidade e a determinação de limites à sua utilização, por um período máximo de 30 dias, além dos passos a adotar, de forma a garantir que esta medida, de vigilância, será mínima.

A *Rule 41* das FRCP (*Federal Rules of Criminal Procedure)* veio a ser alterada, em 2016, nela sendo introduzida uma regulamentação específica para as pesquisas em dispositivos informáticos e para as apreensões de dados informáticos armazenados em tais dispositivos realizadas de forma remota, o que sustenta a ideia de que a admissibilidade do uso do *malware* se encontra prevista nesta disposição. Contudo, a lei não define o que se entende por busca para "acesso remoto", suscitando a questão de se,

[221] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 328.

com esta alteração, se pretendeu confirmar a previsão do *malware* no âmbito da referida R41[222], terminando com a utilização que era feita sem sustentação legal.

Portanto, partindo desta posição, está a situação de "vários mandados de busca, em que se utilizava o *malware*, eram declarados inválidos, como base em aspetos formais"[223], o que levou o legislador a consagrar a busca remota e, também, o alargar do campo de aplicação, face àquilo que seria permitido, ao abrigo da R41[224], afastando desde logo os aspetos que fundamentariam a sua invalidade. Desta forma, seja qual for a posição que se pretenda tomar, isto é, se foi introduzido o *malware* ou apenas se pretendeu alargar o âmbito de aplicação dos mandados de busca, poder-se-á depreender que a "alteração foi substancial ou procedimental/formal"[225].

Quanto ao enquadramento do uso do *malware*, a R 41 determina a necessidade de um mandado de busca, ou seja, uma autorização prévia do juiz do distrito, sendo esse mandado solicitado por um agente federal do governo ou por um procurador[226]. No entanto, a *Rule* não determina qualquer catálogo de crimes. Desta forma, para se saber quando deve ser concedido um mandado de busca para acesso remoto, tem de se atender à 4ª emenda da Constituição, que impõe que deverão ser preenchidos dois pressupostos:

[222] A admissibilidade do *malware*, ao abrigo desta alteração, é criticável, tendo em conta que a R41 está relacionada com investigações de caráter tradicional e, nesse sentido, encontra-se reservada a reger ferramentas de investigação menos invasivas, ou seja, buscas e apreensões físicas em locais físicos. Portanto, não nos parece visível a existência de similitude entre as buscas no local físico e a busca remota, entendida como o uso de *malware*. Assim, acompanhamos a posição de Juliana Campos, de que é controverso legitimar a utilização ao abrigo desta R41. Nota 386, CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 114.

[223] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 115.

[224]A nova versão era mais abrangente, tendo sido descrita como uma atualização processual muito necessária, à luz do uso crescente de ferramentas de anonimato e do aumento do crime cibernético multi-jurisdicional. Que visou em especial, conceder aos tribunais jurisdição para emitir mandados de busca remota, quando a localização de um dispositivo, ou dos dados procurados, fosse ocultada com meios tecnológicos, e permite a emissão de mandados de busca remota multi-jurisdicionais, em determinadas circunstâncias. No entanto, esta alteração foi criticada e caracterizada como "ressuscitadora de mandados gerais", asseverando-se que autorizava o "*hacking* em massa" e permitiria amplos poderes de vigilância extraterritoriais ao FBI. Disponível em https://www.justsecurity.org/35136/rule-41-updated-needed/ (consultado em 01/11/2023).

[225]CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 115.

[226] *Idem*, p. 144.

causa provável *(probable cause)"*[227], e particularidade *(particularity)*[228], o que vêm permitir a busca remota.

3. Experiência alemã

Passando para ordenamento jurídico alemão, temos que inicialmente se considerou que uso do *malware* se encontrava legitimado, tendo em conta que as buscas *online* poderiam ocorrer "com base em aplicações extensivas, ou mesmo analógicas, de três normas do ordenamento jurídico alemão: aquelas que autorizavam a apreensão de objetos, com finalidade investigativa (§ 94 Código de Processo Penal alemão – *Strafprozessordnung, StPO),* a de busca domiciliar (§ 102 StPO) e a do monitoramento de telecomunicações (§ 100a StPO)"[229].

Sucede que, no ano de 2006, no decurso de uma investigação relacionada com terrorismo, foi solicitado um mandato judicial, pelo Ministério Público, a autorizar uma busca remota ao computador do suspeito, por meio da instalação de um tipo de *malware*. Este pedido foi rejeitado a 25 de novembro do mesmo ano e o procurador recorreu ao Tribunal Federal Alemão de Justiça (*Bundesge- richtshof),* argumentando que as disposições incluídas no código de processo penal alemão[230], supracitado, admitiriam a utilização daquele meio de obtenção de prova, uma vez que se estaria perante uma medida processual essencialmente análoga à busca em locais físicos.

---

[227] O conceito de "causa provável" não existe. Nem a quarta Emenda, nem as disposições legais federais, definem "causa provável"; a definição é uma construção inteiramente judicial. O requerente de um mandado deve apresentar ao magistrado factos suficientes para que o próprio agente possa determinar a causa provável. Disponível em https://www.govinfo.gov/content/pkg/GPO-CONAN-REV-2016/pdf/GPO-CONAN-REV-2016.pdf (consultado a 01/11/2023).

[228] O agente deve informar o objetivo do mandado, o que consiste em "descrever a localização da busca, e as pessoas ou as coisas a serem apreendidas". Quarta emenda da Constituição. Contudo, não são raras as vezes, que o *malware* é utilizado com o fito de identificar a localização e as pessoas e, assim sendo, o requisito da particularidade não estaria preenchido, o que levou à criação de mandatos antecipatórios. nota 400, CAMPOS, *Juliana* Filipa Sousa, *O malware* (…), op. cit. p. 118.

[229] *Idem*, p. 110.

[230] GIUSEPPE Vaciago, *Digital Forensics, Italian Criminal Procedure and Due Process Rights in the Cyber Age* (Torino: G. Giappichelli Editore, 2012), 125; RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 216.

O Tribunal Federal nega provimento e conclui que tal analogia não é defensável, fundamentando que o uso desta medida carecia de base legal, tornando-a assim, inadmissível, nos procedimentos dos processos penais[231].

Volvidos trinta dias desta decisão, a 20 de dezembro de 2006, a Lei de Proteção da Constituição da Renânia do Norte foi alterada, vindo-se a introduzir a disposição, no artigo § 5.2 (11), de conceder à entidade responsável pela proteção da Constituição[232] (*Bundesamt für Verfassungsschutz*) o poder de adotar medidas para a obtenção de informações, traduzidas numa monitorização/vigilância secreta, acompanhada doutras ações de reconhecimento da *internet*, incluindo a participação encoberta em *chats* e, embora esta solução seja menos clara, permitindo o acesso ao *email* ou a *websites* de acesso restrito, usando-se credenciais colhidas de diversas fontes[233], para tudo isto se argumentando que as disposições incluídas no código de processo penal alemão[234], supra-citado, admitiriam a utilização daquele meio de obtenção de prova, uma vez que se estaria perante uma medida processual (essencialmente) análoga à busca em locais físicos.

Esta Lei veio possibilitar o acesso aos sistemas informáticos, através da utilização de técnicas que exploram as vulnerabilidades com instalação de *malware*[235], permitindo às autoridades monitorizar, analisar o conteúdo e controlar os sistemas informáticos afetados. No entanto, a aplicabilidade desta medida está sujeita às funções da autoridade de proteção da Constituição, como previsto no § 3 da Lei de Proteção Constitucional da Renânia do Norte-Vestfália[236].

Com a entrada em vigor desta lei, não tardou a que o Tribunal Constitucional Federal fosse convocado para a sua apreciação, quanto à conformidade constitucional

---

[231] *Judgment of the Third Criminal Chamber of the Federal Supreme Court of 31 January 2007, BGH StB* 18/06, available ahttp://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=200 7-1&nr=38779&pos=11&anz=268 (consultado em 28/10/2023).

[232] https://www.bmi.bund.de/EN/topics/security/protection-of-the-constitution/protection-ofthe constitution.html (consultado em 28/10/2023).

[233] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 217.

[234] GIUSEPPE Vaciago, *Digital Forensics, Italian Criminal Procedure and Due Process Rights in the Cyber Age* Torino: G. Giappichelli Editore, 2012, 125; RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 216.

[235] O tribunal declarou que «[tais] medidas já foram executadas em casos isolados, por autoridades federais, sem fortalecimento da legislação específica. Pouco se sabe da natureza da execução prática de "pesquisas on-line" anteriores, ou de seus resultados', Julgamento do Primeiro Senado, de 27 de fevereiro de 2008, com base na audição oral de 10 de outubro de 2007, 1 BvR 370, 595/07.

[236] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 217.

como, também, quanto ao uso deste meio de obtenção de prova, o que viria a suceder em 27 de fevereiro de 2008, vindo ele a declarar a inconstitucionalidade do §5.2. da lei de proteção da Constituição da Renânia do Norte-Vestefália, por violar o direito fundamental à integridade e confidencialidade dos sistemas, e os princípios da clareza e da proporcionalidade[237]. Não obstante, fê-lo, fornecendo as orientações para uma nova formulação legal para o uso deste meio de obtenção de prova, "em conformidade com os imperativos constitucionais violados".

Levando em consideração os comentários construídos pelo Tribunal Constitucional Federal, não para o propósito de processo criminal, mas apenas para fins de prevenção[238], surge a admissibilidade do uso de *malware* em casos de terrorismo internacional, sendo ela introduzida expressamente na lei alemã através do *Bundeskriminalamt (Gesetz zur Abwehr von Gefahrendes des internationalen terrorismos durch das Bundeskriminalamt*), de 25 de dezembro de 2008, fixando o recurso ao *malware* a título muito excecional.

4. Experiência espanhola

No ordenamento jurídico espanhol, até ao ano de 2015, a investigação criminal tecnológica era regida pelas disposições legais do processo penal de 1881, as quais não sofreram reforma durante décadas[239].

As alterações da LO13/2015, de 5 de outubro, vieram introduzir algumas medidas na LECrim, que, através dos artigos 588 bis a 588 octies, apresentaram uma "extensa e

[237] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. pp. 329 e 217-218.
[238] Klaus Rogall, 'A nova regulamentação da vigilância das telecomunicações na Alemanha', in Maria Fernanda Palma and others, AA.VV., 2.º Congresso de Investigação Criminal, Coord., (Coimbra: Almedina, 2009 pp. 177-220.
[239] Por ex., a regulamentação das intervenções telefónicas da revisão de documentos. Nesse sentido, VELASCO NÚÑEZ, Eloy, Aspectos procesales de la investigación y de la defensa en los delitos informáticos. Em La Ley: Revista Española de Doctrina, Jurisprudencia y Bibliografía. N.º 6506. Ano 2006 e MAGRO SERVET, Vicente, La instrucción de los delitos informáticos. Em Estudios de Derecho Judicial. La instrucción de los delitos económicos y contra la hacienda pública. Ed. Consejo General del Poder Judicial (Madrid) 2005. URIA. Disponível em https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877&forceDownload=true. (consultado em 12/03/2024).

exaustiva regulamentação processual da ciber-investigação". Os "*registros remotos sobre equipos informáticos*" estão previstos nos artigos 588 spties a, b e c da LECrim[240].

Estas disposições passaram a determinar que o "juiz competente poderá autorizar a utilização de dados de identificação e códigos, bem como a instalação de programas informáticos/*softwares* que, remotamente e por via telemática, permitam o exame à distância, sem o conhecimento do seu utilizador, do conteúdo de um computador, de um dispositivo eletrónico, de um sistema informático, ou de um instrumento informático de armazenamento de dados"[241] . Desta forma e com esta medida, o legislador, em primeiro lugar, distinguiu dados de identificação e códigos utilizados para aceder remotamente ao sistema informático e, por outro, autorizou/viabilizou a instalação do *software*[242], o que se traduz na legitimação do *hacking* e do *malware*.

Assim sendo, a reforma veio harmonizar as questões referentes à "intervenção e acesso a comunicações telemáticas, desde os dados das comunicações até aos de conteúdo, dispositivos de armazenamento, captação de voz ou imagem e, em suma, qualquer elemento probatório de natureza tecnológica que possa ser útil para efeitos de investigação"[243].

No entanto, quaisquer destas medidas estão subordinadas ao princípio da especialidade, tendo em conta o alcance aos direitos fundamentais. A investigação criminal deverá ter "por objeto o esclarecimento de um facto punível concreto, proibindo-se expressamente a investigação prospetiva. E dever-se-ão satisfazer os princípios de idoneidade, excecionalidade, necessidade e proporcionalidade, na ocorrência, que deverá estar suficientemente justificada na comunicação judicial, para esses efeitos"[244]. Apenas serão, tais medidas, permitidas para um grupo particular de crimes graves, como o terrorismo, crimes contra menores ou pessoas com capacidade modificada judicialmente,

[240] NUNES, Duarte Rodrigues,.*Os meios de obtenção* (…), op. cit. p. 484.
[241] Artículo 588 septies a. Da *Ley de Enjuiciamiento Criminal española*
[242] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 326.
[243] Proença de Carvalho, F., Morales García, O., & Álvarez Feijoo, M. (2018). Regulamentação supranacional sobre criminalidade informática e técnicas de transposição: o Direito penal português e espanhol como paradigmas. *Regulamentação supranacional sobre criminalidade informática e técnicas de transposição: o Direito penal português e espanhol como paradigmas*, pp. 62-63. https://vlex.es/vid/regulamentacao-supranacional-criminalidade-informatica-741779885 (consultado em 28/03/2024).
[244] *Idem*, p. 63.

crimes contra a Constituição, de traição e para qualquer crime cometido através de instrumentos informáticos ou de qualquer tecnologia de informação ou comunicação.

A nova lei também determina o dever de colaboração de prestadores de serviços, ou seja, de terceiros, de telecomunicações e sociedades de informação. Nestes casos, com o limite de "duração inicial de um mês", prorrogável até três meses. De igual forma, será necessária a conservação de dados ou informações incluídas num determinado sistema informático de armazenamento, até que se obtenha a autorização judicial correspondente[245].

5. Outras experiências

Em França, o uso investigativo de *malware* foi consagrado na reforma ao código de processo penal, levada a cabo pela Lei nº 2011-267, de 14/03/2011, sendo introduzido na secção 6 bis, sob a epigrafe "captura de dados informáticos", nos artigos 706- 102- , a 706- 102- 9[246].

A necessidade do uso de *malware* está essencialmente relacionada com os crimes abrangidos pelo artigo 706 73, como a criminalidade praticada de forma organizada, crimes de homicídio, tráfico de droga, roubo. As operações são realizadas sob a autoridade e controlo do juiz de instrução. O JI pode autorizar o MP, caso em que este, por despacho fundamentado, deve fazer constar, sob pena de nulidade, o motivo do recurso a este meio, a referência à localização exata ou a descrição detalhada dos sistemas informáticos e a duração da operação, que será, no máximo, de quatro meses, renovável por igual período.

No caso da Finlândia, o artigo 26 do capítulo 10 da Lei n.º 806/2011[247], a designada Lei das Medidas Coercitivas, vem permitir, na investigação criminal, a possibilidade de se instalar um dispositivo, procedimento ou programa, num sistema informático, para "fins de vigilância técnica", assim se entrando dissimuladamente no

[245] Esta disposição vem transpor de forma quase literal, o artigo 16º da Convenção de Budapeste sobre a conservação expedita de dados informáticos armazenados.
[246] https://www.legifrance.gouv.fr/codes/id/LEGISCTA000023712495/2011-03-16 (consultado em 28/03/2024).
[247] https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf (consultado em 28/03/2024).

sistema de modo a contornar, desinstalar ou, de forma correspondente, evitar ou dificultar temporariamente a proteção dos objetos ou do sistema de informação. Encontra-se também "prevista a utilização do dispositivo do suspeito para a gravação de som e imagem e para obtenção de informação sobre a geo-localização"[248].

Na União Europeia, também se procurou incrementar a consagração do *malware* como meio de obtenção de prova em todo o espaço europeu.

Assim, em 2008, na tentativa de adoção de estratégias para reforçar o combate ao cibercrime, o Conselho de Ministros da União Europeia comunicou a sua estratégia, que incluiria o recurso a uma "ciber-patrulha" para localização em rede de criminosos e pequenas pesquisas remotas, entre outras ações.

Mais tarde, em 2011, a União Europeia faria constar no seu considerando n.º 27, a Diretiva 2011/92/EU do Parlamento Europeu e o Conselho da Europa, de dezembro de 2011, sobre o combate ao abuso sexual e à exploração sexual de crianças e pornografia infantil, com a seguinte previsão: "os responsáveis pela investigação e pela ação penal relativos aos crimes referidos na presente diretiva deverão dispor de instrumentos de investigação eficazes. Estes instrumentos podem incluir a interceção de comunicações, a vigilância direta, inclusive por meios eletrónicos, a monitorização de contas bancárias, ou outras investigações financeiras, tendo em conta, nomeadamente, o princípio da proporcionalidade e a natureza da gravidade dos crimes investigados. Se for caso, e de acordo com a legislação nacional, tais instrumentos deverão também incluir a possibilidade de as autoridades policiais utilizarem identidades falsas, na *Internet*." [249].

6. Em Portugal: a suposta aquisição do *software* pela PJ e a *Cellebrite*

No espaço português, em 2018, corria a notícia, pela comunicação social, da possível aquisição, pela PJ, de um certo *software.* Tal programa viria permitir a "aquisição remota de prova digital em 'terminais de comunicações móveis' ou, por outras palavras, tratar-se-ia de um "sistema informático com ferramentas que permitem fazer a

[248]RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. pp. 336

[249] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:PT:PDF, p. 4 (consultado em 28/03/2024).

recolha de dados de dentro de telemóveis (em especial, *smartphones*), à distância"[250]. Seria uma despesa importante, custando ao Estado cerca de 2,9 milhões de euros, autorizada pelo Governo e, pois, permitiria à Polícia aceder a telemóveis de suspeitos à distância[251].

A aquisição deste *software* teve como finalidade dotar a PJ dos "meios técnicos adequados à promoção e reforço da prevenção e da repressão da criminalidade transnacional grave e organizada, designadamente o terrorismo, o tráfico de seres humanos, o cibercrime, o tráfico de droga e o crime económico-financeiro, ao tempo se fomentando a cooperação, quer com os restantes Estados-Membros, quer com Países Terceiros"[252].

Apesar do processo de aquisição do referido *software*, que se previa concluído nos meses seguintes, prontamente parece ter sido olvidado, não tendo havido posteriores referências ao mesmo. No entanto, foram suscitadas dúvidas quanto à sua legalidade.

Apartando a questão da aquisição do sistema, importa saber qual o suporte legal que permitiria a utilização do mesmo, e se a recolha de dados poderia ser feita cumprindo os "procedimentos legais".

Como referido, este sistema permite a aquisição remota de prova digital em "terminais de comunicações móveis"[253]ou, por outras palavras, possibilita a recolha de dados dos telemóveis, remotamente e sem o conhecimento do suspeito. A ser assim, estaríamos perante um programa insidioso que possibilitaria a obtenção de dados, elementos de prova que "existem dentro dos equipamentos móveis de suspeitos da prática de crimes"[254].

Em face do que acima se disse resulta, nesta fase, evidente que o uso do *malware* não se encontra consagrado no ordenamento jurídico português e, portanto, a aquisição

[250] SIMÕES, Bruno, "PJ vai comprar software para extrair dados de telemóveis à distância", in Jornal de Negócios, 03/01/2018, disponível em https://www.jornaldenegocios.pt/economia/defesa/detalhe/pj-vai-comprar-software-para-extrair-dados-de-telemoveis-a-distancia (consultado a 11/03/2024).
[251] Diário da República n.º 2/2018, Série II de 03-01-2018, p. 164, disponível em (consultado a 11/03/2024).
[252] *Idem*.
[253] SIMÕES, Bruno, "PJ vai comprar software para extrair dados de telemóveis à distância", in Jornal de Negócios, 03/01/2018, disponível em https://www.jornaldenegocios.pt/economia/defesa/detalhe/pj-vai-comprar-software-para-extrair-dados-de-telemoveis-a-distancia (consultado a 11/03/2024).
[254] *Idem.*

deste *software* pela PJ encaminhar-nos-ia a averiguar se ele seria admissível, como meio de prova[255].

Em 2021, o assunto volta à ribalta na comunicação social, com a notícia, de que a "PJ, o Serviço de Estrangeiros e Fronteiras e a Guarda Nacional Republicana compraram as ferramentas da polémica empresa Cellebrite, que permitem aceder a, e extrair informações de equipamentos eletrónicos, incluindo smartphones protegidos por código de bloqueio"[256].

A Cellebrite é uma empresa israelita, especializada em tecnologias de investigação forense, que ficou conhecida por comercializar "ferramentas" que permitem aceder a, e extrair dados dos smartphones bloqueados, sendo o seu programa *"Universal Forensic Extraction Device* (UFED)[257]" o mais comentado[258].

O UFED permite aceder a smartphones ainda que bloqueados, recolher informações, mensagens, e-mails, registos de chamadas, fotografias, localizações e até recuperar alguns ficheiros já apagados [259].
O que está agora em causa é saber se o uso deste programa tem acolhimento no ordenamento jurídico português. Partindo do princípio de que, no decurso do inquérito, foi efetuada a apreensão de um equipamento informático, a mesma tem de ser validada por despacho da AJ, conforme disposto no artigo 178º do CPP.

Sendo depois autorizada, pela AJ competente, a pesquisa de dados informáticos, nos termos do artigo 15º da LC, para recolha de dados específicos e determinados, contidos no equipamento, necessários à produção de prova, tendo em vista a descoberta da verdade, ela deve conter-se num prazo de validade máximo de 30 dias.

---

[255] Importa referir que nada se sabe, quanto ao uso deste sistema pela PJ, no âmbito da investigação.
[256] PEREIRA, Rui da Rocha, "PJ, SEF e GNR compraram polémico *software* israelita para aceder a smartphones bloqueados", in Sapo Visão, 06/05/2021, disponível em https://visao.pt/exameinformatica/noticias-ei/mercados/2021-05-06-pj-sef-gnr-cellebrite-portugal-codigo-azul/ (consultado em 15/03/2024).
[257] Universal Forensic Extraction Device (UFED) – em tradução livre significa 'dispositivo universal de extração forense'.
[258] PEREIRA, Rui da Rocha, "PJ, SEF e GNR compraram polémico *software* israelita para aceder a smartphones bloqueados", in Sapo Visão, 06/05/2021, disponível em https://visao.pt/exameinformatica/noticias-ei/mercados/2021-05-06-pj-sef-gnr-cellebrite-portugal-codigo-azul/ (consultado em 15/03/2024).
[259] *Idem*.

Segue-se, então, a apreensão de dados informáticos, conforme o artigo 16.º da LC, apreensão que consiste em a AJ colher para o processo dados informáticos que se encontrem num sistema informático ou suporte autónomo, na decorrência da diligência.[260]

A ser assim, o uso do programa UFED, para recolha de dados que (sejam) fossem determinantes à descoberta da verdade, no equipamento apreendido, estar-se-ia no âmbito da apreensão de dados informáticos, um meio de obtenção de prova idóneo.

Feito o contexto deste software nas disposições legais acima referidas, concluímos que a utilização daquele não se confunde com o uso *malware* no âmbito da investigação criminal. Uma vez, que programa UFED se destinada a fazer a extração de dados, pelas autoridades competentes e autorizado pela AJ. Ao passo que o *malware*, é instalado de forma oculta, permitindo o acesso ilimitado, à recolha de dados armazenados, ou o acompanhamento da atividade do utilizador em ambiente digital em tempo real, inclusive com a ativação de funcionalidades de *hardware* como" GPS, câmara e microfone"[261].

Em suma e em síntese apertada, em relação aos casos divulgados, resta-nos dizer que nada mais tem sido referenciado pela comunicação social, pelo que se suscita a dúvida quanto ao uso destes instrumentos pelas autoridades competentes, no âmbito da investigação criminal. Sublinhemos que o programa UFED, adquirido à empresa Cellebrite, permite que seja feita uma extração de dados que podem vir a ser determinantes para a descoberta da verdade, extração que, de outra forma, seria muito difícil ou impossível.

[260] NUNES, Duarte Rodrigues. *Os meios de obtenção* (…), op. cit. p.261

[261] O uso do *malware* na investigação criminal pontos de tensão e limites do *malware* disponível DOI: https://doi.org/10.5281/zenodo.10188525 , (consultado em 17/03/2024).

CAPÍTULO V: REQUISITOS PARA A ADMISSIBILIDADE DO *MALWARE* NO ORDENAMENTO JURÍDICO PORTUGUÊS

1. Requisitos para a admissibilidade

A evolução e a proliferação das tecnologias de informação e comunicação, aliadas à rapidez e à facilitação do anonimato em ambiente digital, vieram causar grandes dificuldades à investigação criminal e, por via disso, suscitar questões quanto à matéria de recolha de prova.

Tendo em conta a mudança para uma criminalidade mais complexa, as autoridades judiciárias obrigam-se a estar dotadas das mesmas vantagens tecnológicas utlizadas pelos criminosos, emergindo assim a necessidade de se criarem novos métodos de investigação. É neste contexto que reconhecemos a indispensabilidade do uso do *malware* na descoberta da verdade, dado o seu elevado potencial de recolha, inexistente noutro qualquer meio de obtenção de prova.

Por outro lado, como já abordado, observamos que o *malware* é um meio de recolha de prova de elevada "danosidade social", "intrusivo e intensamente restritivo de direitos fundamentais"[262] consagrados na nossa lei processual penal. De facto, com o uso de um programa insidioso para o investigar, o utilizador do sistema informático pode ter os seus direitos, bem como os de terceiros, restringidos, que varia em função da "concreta funcionalidade utilizada"[263].

Assim, nas próximas linhas, pretendemos abordar alguns requisitos formais, materiais e orgânicos, que consideramos indispensáveis, os quais devem ser atendíveis, quando da operabilidade da concordância prática, a fim de que o uso do *malware* seja legal e constitucionalmente admissível.

[262] RAMALHO, David Silva, *Métodos Ocultos* (…) op. cit. p. 351.
[263] CAMPOS, *Juliana* Filipa Sousa, *O malware* (…), op. cit. p. 155.

2. Requisitos formais

Como referimos, o uso do *malware* pode restringir um conjunto de direitos constitucionalmente garantidos e protegidos, daí a usual exclusão liminar da admissibilidade deste método oculto e a consequente imposição de uma "intransponível exigência da reserva de lei"[264]. Assim, consideramos como primeiro pressuposto, a necessária habilitação legal expressa, impondo-se uma lei da "Assembleia da República ou um decreto-lei autorizado do governo", que execute a requerida previsão legal e a "densificação do regime jurídico" aplicável, *ex vi* n. º2 do artigo 18º e do artigo 165º n. º1, alínea b). da CRP, "condição fundamental da legitimidade e da validade da prova obtida"[265]. Uma lei, então, que permita "identificar com rigor e segurança, tanto o bem jurídico ou o direito fundamental lesado ou atingido, como o teor do respetivo sacrifício"[266].

O regime jurídico dos instrumentos em discussão deverá estar previsto na lei de forma independente da dos outros meios ocultos de obtenção de prova, passando essa previsão a se encontrar nas "normas que regulam a prova digital"[267].

Enquadrando-se o *malware* nos métodos ocultos, torna-se determinante que o legislador proceda à sua previsão "de forma expressa, e claramente,"[268] vinculando as

---

[264] ANDRADE, Manuel da Costa, *Métodos ocultos de investigaçã*o *(Pläydoyer para uma teoria geral). AAVV, Que futuro para o Direito Processual Penal?* Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português. Coimbra: Coimbra Editora. 2009. p. 540;
RAMALHO, David Silva, *Métodos Ocultos* (…) op. cit. p. 216; CAMPOS, Juliana, A investigação oculta em ambiente digital: a utilização de *malware* / *Revista Portuguesa de Ciência Criminal,* RPCC, Lisboa, Ano 32, n.º 1 (janeiro-abril 2022), p. 193. A propósito de reserva de lei *vide* nº 1do art.º 52 da CDFUE que afirma que "qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos"

[265] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 220.

[266] LOPES, Sónia Raquel da Cruz. Interceção de comunicações para prova dos crimes de lesões, ameaças, coação, devassa da vida privada e perturbação da paz e do sossego, cometidos por meio diferente do telefone. *Revista da Concorrência e da Regulação,* Ano VII • Número 29 janeiro – março 2017. p. 240.

[267] CAMPOS, Juliana, A investigação oculta em ambiente digital: RPCC, Lisboa, Ano 32, n.º 1 (janeiro-abril 2022). p. 193. A prova digital no nosso ordenamento jurídico "está, hoje em dia, regulada em três diplomas legais: o Código de Processo Penal, a Lei n.º 32/2008, de 17 de julho (que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas) e, ainda, a Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime)" CORREIA, João Conde Revista do Ministério Público 139: julho : setembro 2014. p. 24.

[268] ANDRADE, Manuel da Costa. *Métodos ocultos de investigação* (…) op. cit. p. 540; RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 221. Impedir o livre arbítrio das atuações das autoridades publicas, fazer a sujeição ao regime legal e, por outro lado, permitir um controlo jurisdicional efetivo, pelo que se torna necessário que esta lei preveja "expressa e claramente a medida de compressão dos direitos fundamentais, fixando a compressão, a extensão e a vinculação finalístico-teleológica bem como a definição dos limites".

finalidades e a definição dos limites, o que, segundo a jurisprudência alemã, se denomina por "princípio da vinculação ao fim", isto é, deve ser indicado o fundamento, o fim e os limites da interceção, de uma forma precisa e clara,[269] respeitando-se "o princípio da precisão e da determinabilidade dos atos normativos"[270].

Portanto, as expressões vagas e indeterminadas, ou demasiado abrangentes, como "meios técnicos" ou "meios de dispositivos informáticos", devem ser arredadas, tal como as denominações semelhantes a outros meios de prova, já existentes na legislação processual, como buscas ou pesquisas on-line[271], devendo prevalecer, no nosso entender, *de iure condendo,* a designação de *malware*, pelos seguintes motivos: "i) corresponde ao termo técnico consagrado; ii) contribui para uma segurança jurídica e proteção da confiança dos cidadãos, pois, segundo a doutrina, a jurisprudência e o legislador noutros ordenamentos jurídicos e o nosso" , perfilham diferentes designações para se referir ao *malware*; iii) a "terminologia em língua inglesa não constitui óbice à sua integração no ordenamento jurídico português" tendo em conta a existência de outros diplomas legais que não foram objeto de tradução para a língua portuguesa, não obstante o artigo 10.º n.º3 da CRP; e iv) para finalizar, no "Guia prático das regras a observar na redação dos atos normativos da Assembleia da República" são visíveis algumas exceções na utilização da língua portuguesa, figurando entre elas certos termos de elevado índice técnico, para os quais não há ainda expressão consagrada na nossa língua.

Assim, caso se pretenda traduzir o termo *malware* a designação que preconizamos é a de "programa informático malicioso", tratando-se da tradução[272] bastante fiel daquele vocábulo.

[269] LOPES, Sónia Raquel da Cruz. Interceção de comunicações para prova dos crimes de lesões, ameaças, coação, devassa da vida privada e perturbação da paz e do sossego, cometidos por meio diferente do telefone. RCR. p. 240.
[270] CAMPOS, Juliana, A investigação oculta em ambiente digital: a utilização de *malware* / *Revista Portuguesa de Ciência Criminal*, RPCC, Lisboa, Ano 32, n.º 1 (janeiro-abril 2022), pp. 193-194.
[271] CAMPOS, Juliana, A investigação oculta em ambiente digital: a utilização de *malware* / *Revista Portuguesa de Ciência Criminal*, RPCC, Lisboa, Ano 32, n.º 1 (janeiro-abril 2022), p. 194.
[272] Reconhecemos que as traduções podem acarretar riscos de falta de precisão e de demarcação do concreto sentido.

Por último, optando-se por denominações existentes na nossa língua, considerámos que, o artigo deve conter uma "menção expressa a instalação do software/programa informático sem o conhecimento do utilizador"[273].

3. Requisitos materiais

Após a consagração do *malware* na lei, impõem-se algumas exigências, quanto às condições e limites da sua aplicabilidade, enquanto meio oculto de obtenção de prova, pelo que o legislador deverá determinar o tipo de crime para o qual será permitido o uso de *malware*, relevando o carácter excecional e não automático e, pois, sendo o recurso a este meio uma *ultima ratio*[274].

Assim, partimos da questão de se seria o bastante uma norma de forma genérica, com remissão para o regime geral, para a admissibilidade do uso *malware*. Realmente, não nos parece o bastante, e rejeitamos que uma norma genérica confira supedâneo legal suficiente à utilização de *malware*.

Contudo, dentro dos meios ocultos de obtenção de prova, o recurso a esta medida, em *ultima ratio,* não deve ser seguida de uma remissão genérica "naquilo que for aplicável" para um regime legal que, por sua vez, remete "em tudo o que não for contrariado" para outro regime. Ademais, dado o elevado alcance deste meio e o seu grau de lesividade, a sua admissibilidade não poderia ficar ao abrigo de qualquer preceito já previsto na lei[275].

Também não nos parece aceitável por que norma genérica ou catálogo de crimes possa ele ser reconduzido para um regime de outros meios de obtenção de prova já previstos no nosso ordenamento, como por exemplo o regime das escutas telefónicas[276],

---

[273] CAMPOS, *Juliana* Filipa Sousa, *O malware* (…), op. cit. p. 158.
[274] Ao inverso do que se observa nos EUA, R41 b 6.
[275] O TEDH, nesta matéria, para cumprimento dos requisitos impostos pelo artigo 8.º da CEDH, determina que não basta a existência de previsão legal, é necessária a uma imposição de "qualidade da lei" que torne as medidas processuais acessíveis e previsíveis, de modo que o cidadão possa conhecer as condições, limites e circunstâncias em que as mesmas podem ser aplicadas. 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. out - dez. de 2013. p. 233- 234.
[276] Encarámos o regime das escutas telefónicas "como meio de obtenção de prova particularmente intrusivo, caracterizando-se pela intromissão na intimidade da vida privada e familiar, na correspondência e na comunicação por meio da palavra falada, e acarretando, por isso, uma elevada e expandida danosidade

sendo materialmente bem distintos[277] e, portanto, deve ser feita mais restrita a utilização de *malware*.

Desta forma, em primeiro lugar, consideramos necessária a criação de um catálogo específico, com especial incidência em crimes suficientemente graves, ou crimes que possam representar um grave perigo para a comunidade, respeitando-se o princípio da proporcionalidade, ou seja, um regime jurídico rigoroso, com catálogo autónomo de crimes, tornando-se inaplicável este meio de obtenção de prova a outro tipo de crimes.

Segundo, insuficiente também se nos apresenta a recondução da factualidade ao catálogo de crimes, impondo-se a observação de uma "suspeita fundada" em factos "concretos e medidos com critérios de plausibilidade e probabilidade"[278], havendo até "um certo nível de indícios"[279] a considerar. Para além de que, com o uso do *malware*, podem ser recolhidas provas da prática de um crime, o que permitirá facilmente avançar

social. Do ponto de vista desses direitos fundamentais, essas escutas estão conectadas , de modo particularmente intenso, com o regime das proibições de prova, nas modalidades de proibição de produção e ou de utilização. «*Não fossem os condicionalismos rigorosos que o tornam admissível, dir-se-ia ser mesmo um meio de obtenção de prova desleal, contrário ao cerne do processo penal*»" LOPES, José Mouraz, «Escutas telefónicas: seis teses e uma conclusão», Revista do Ministério Público, Ano 126, n.º 104– Out/Dez 2005) Ac.TRL n.º 40/18.3 JAPDL-A. L1-5, Relator Cid Geraldo. Contudo, a instalação do *malware* no sistema informático do suspeito, para obtenção de prova, é um meio muito mais intrusivo, possivelmente o meio mais gravoso de obtenção de prova, de superior danosidade social, quando comparado com o regime das escutas telefónicas, tendo em conta a "monitorização remota da conduta privada de um indivíduo no seu computador", possivelmente acompanhada da captação de imagens e som do visado com recurso ao mesmo sistema informático, numa intromissão potencialmente inadmissível no núcleo intangível da intimidade pessoal. 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. out. - dez. de 2013. p. 233.

[277] CAMPOS, Juliana, A investigação oculta em ambiente digital: a utilização de *malware* / *Revista Portuguesa de Ciência Criminal*, RPCC, Lisboa, Ano 32, n.º 1 (janeiro-abril 2022), p. 196.

[278] LOPES, Sónia Raquel da Cruz, Interceção de comunicações…. op. cit. p. 241.

[279] Não basta uma mera suspeita, mas sim a "exigência de uma suspeita fundada da prática de certo crime do catálogo; Parece que 'fundada suspeita' pressupõe que já haja um certo nível de indícios; logo, não basta a mera 'notícia do crime' e, muito menos, uma denúncia anónima, mesmo que muito verosímeis e suficientemente concretizadas e que iii) uma utilização prática subsidiária do *malware*, ??o que vale por dizer que só se mostra admissível o recurso a este meio intrusivo se não for possível alcançar "a mesma eficácia probatória à custa de meios menos gravosos". Carlos Adérito Teixeira in *"Escutas Telefónicas: A Mudança de Paradigma e os Velhos e os Novos Problemas" (Revista do CEJ, Número 9, págs. 244-245 referiu exemplarmente o seguinte: «Leio a atual formulação do n.º 1 do art. 187º do CPP como representando: i) uma mais exigente ponderação, no plano concreto, sobre a* necessidade, a proporcionalidade, a adequação ou a idoneidade do meio (escuta); Ac. TRE Proc. N.º 2871/17.2T8STR.E1., Nota CAMPOS, Juliana, A investigação oculta em ambiente digital: a utilização de *malware* / *Revista Portuguesa de Ciência Criminal*, RPCC, Lisboa, Ano 32, n.º 1 (janeiro-abril 2022). p. 196.

de uma suspeita para uma certeza e, a ser assim, requer-se "que aquela seja aferida no momento em que a autoridade competente decide a autorização ou a recusa da medida"[280].

Em terceiro lugar, outro pressuposto que nos parece relevante é o da multiplicidade de funções que o *malware* comporta, o que nos leva a considerar indispensável a delimitação do seu âmbito funcional, ou seja, as funções para as quais se destinará, concretamente. Assim, entendemos que deve apenas ser usado para aceder a dados armazenados, a dados produzidos em tempo real, ou a ambos e, se comportar a possibilidade, de ativar o *hardware* para esses fins.

Por outro lado, o legislador deve estabelecer critérios distintos, mais rigorosos, caso o *malware* seja instalado num domicílio, um direito constitucionalmente consagrado, pois, como sabemos, uma das funcionalidades do programa informático é a de se ativar a imagem e o som, para recolha de prova externa. Caso não seja possível conhecer a localização, "apenas deve ser admissível a utilização de *malware* se este somente comportar funcionalidades de recolha de prova interna"[281], salvaguardando o núcleo da intimidade do suspeito e de terceiros, ficando assim afastadas eventuais dubiedades.

Quanto à delimitação temporal do uso de *malware*, quarto requisito, cabe-nos dizer que o legislador deverá determinar a duração, isto é, o tempo limite máximo para a execução desta medida, devendo a mesma duração ser estabelecida proporcionalmente, ou seja, por um determinado período que não exceda o de outros meios de obtenção de prova, menos invasivos e já consagrados na nossa lei[282]. Quanto à contagem do prazo, ela deve ser iniciada no momento da instalação, e não quando o juiz emite a sua autorização, mas deve existir um "acompanhamento judicial da efetivação da operação"[283].

Em quinto lugar, consideramos que o legislador deverá prever medidas que assegurem o respeito pelo princípio do contraditório, tratando-se este de uma das garantias de defesa que o processo criminal confere ao arguido, conforme art.º 32.º n.1 da

[280] CAMPOS, Juliana, A investigação oculta em ambiente digital: a utilização de malware / *Revista Portuguesa de Ciência Criminal*, RPCC, Lisboa, Ano 32, n.º 1 (janeiro-abril 2022), p. 196-197.
[281] *Idem*, p. 198.
[282] CAMPOS, *Juliana* Filipa Sousa, *O malware* (…), op. cit. pp. 164-165.
[283] Acompanhamos a posição de CAMPOS, *Juliana* Filipa Sousa. A investigação oculta em ambiente digital: op. cit. p. 198.

CRP [284]. Portanto, uma vez que o *malware* é instalado sub-repticiamente, torna-se determinante o controlo da sua fiabilidade e integridade, e da sua a aplicabilidade ao caso concreto. Assim, o juiz, no despacho que autoriza a intervenção, deve fazer constar o tipo de programa malicioso a ser utilizado e quais as funcionalidades ativadas. De outra forma, o arguido ficaria impedido de defender a sua posição e contrariar a acusação[285]. Repare-se que a pessoa visada desconhece por completo a ingerência no seu sistema informático, não sabe a forma como a prova foi recolhida nem, muito menos, que tipo de *malware* foi utilizado, pelo que a sua defesa está comprometida. Para garantir o pleno contraditório, impõe-se uma previsão de medidas que acautelem a integridade e a autenticidade das provas recolhidas, contribuindo para o exercício dos direitos de defesa do visado. Que assegurem que a informação recolhida não sofreu qualquer alteração, seja de forma propositada, seja acidental [286].

Por último, de acordo com a provisão do artigo 18º, n.º 2 da CRP, o princípio da proporcionalidade assume nesta matéria uma dupla dimensão. Este princípio deve estar presente "no conteúdo e no regime" dos vários requisitos materiais de que depende a aplicação do programa informático malicioso. Por outro lado, o julgador terá que, no momento, autorizar ou recusar a sua utilização, de acordo o caso concreto. Sabemos, também, que o princípio da proporcionalidade se desdobra em três subprincípios: a adequação (idoneidade/conformidade), a necessidade (exigibilidade) e a proporcionalidade em sentido restrito.

Assim, a utilização de *malware* aplicado ao caso concreto deverá cumprir o princípio da adequação, o que se traduz numa relação de simbiose entre o programa informático malicioso a utilizar e a persecução da finalidade pretendida, isto é, as provas que se pretende obter, através dele, de um crime previsto no catálogo.

Por outro lado, como já anteriormente mencionado, o *malware* surgirá como meio de obtenção de prova necessário, caso não se observe um outro meio menos restritivo e menos gravoso, com que as autoridades competentes procedam à recolha, mostrando-se,

[284] ANTUNES, Maria João, Direito Processual Penal. 3.ª Edição, Coimbra: Almedina, 2021, p. 86.
[285] O processo criminal assegura todas as garantias de defesa ao arguido. Note-se que a Constituição não limita as garantias de defesa ao arguido, mas alarga-as a todo o processo, e este inicia-se com a abertura do inquérito. SILVA, Germano Marques da. *Direito processual penal português.* Vol. I, Editora Universidade católica portuguesa, Lisboa, 2017. p. 73.
[286] A este respeito, *vide* CAMPOS, *Juliana* Filipa Sousa, *O malware* …, op. cit. pp. 133-136.

desta forma, meio indispensável. Assim, consideramos que no regime jurídico deve constar, de forma expressa, que o recurso a este meio de obtenção de prova só se tornará viável quando não for possível encontrar, no ordenamento jurídico, um outro meio suficiente ao fim que se pretende, ou seja, um meio que responda à necessidade.

Por fim, para o subprincípio da proporcionalidade em sentido restrito, o juiz deverá verificar se a medida é excessiva para o fim que se pretende atingir[287]. O juiz terá de atender ao tipo e extensão dos dados recolhidos, ao tipo de *malware* e respetivas funcionalidades comportadas, e ainda atender questão do tempo de utilização, e só desta forma poderá devidamente aferir o grau de invasão e de restrição de direitos fundamentais, ponderando com a gravidade dos crimes em análise e com a relevância das provas para a investigação[288]. Desta forma, salvaguardar-se-á que o recurso a este meio de obtenção de prova não violará o princípio da proporcionalidade.

No que concerne às exigências do princípio da subsidiariedade, depreendemos que a utilização de *malware* só é permitida quando outros meios de obtenção de prova não permita a recolha de elementos probatórios, isto é, quando os outros meios de prova, "abertos", não sejam suficientemente satisfatórios aos interesses da investigação criminal. Como refere Costa Andrade não é suficiente que a investigação se torne mais difícil sem o *malware,* é essencial que se torne consideravelmente impossível[289].

Posto isto, e em virtude do elevado grau de lesividade e intrusividade que o *malware* pode alcançar, ele deve ser um meio de obtenção de prova de última *ratio,* pelo que não bastará invocar a sua necessária utilização. Assim sendo, consideramos que deve decorrer "do texto da lei, no qual se proceda á sua previsão", deverão estar presentes expressões como "sem a medida, a investigação resulta dificultada, consideravelmente dificultada ou impossibilitada"[290].

---

[287] CAMPOS, *Juliana* Filipa Sousa, *O malware* …, op. cit. p. 165; CAMPOS, Juliana, A investigação oculta em ambiente digital … op. cit. p. 200.
[288] *Idem*.
[289] LOPES, Sónia Raquel da Cruz. Interceção de comunicações para prova dos crimes de lesões, ameaças, coação, devassa da vida privada e perturbação da paz e do sossego, cometidos por meio diferente do telefone. *Revista de Concorrência e Regulação* Ano VII • Número 29 janeiro – março 2017 pp. 240-241; ANDRADE, Manuel da Costa, *Métodos ocultos de investigação* (…), op. cit. p. 550.
[290] CAMPOS, Juliana Filipa Sousa, *O malware* …, op.cit. p.167; CAMPOS, Juliana, CAMPOS, Juliana, A investigação oculta em ambiente digital (…), op. cit. p. 201.

Por último, não podemos olvidar que o *malware* permite o acesso a dados referentes à reserva da vida privada, isto é, à área nuclear da intimidade, os quais devem, pois, ser salvaguardados. Portanto, pretende-se um regime que tenha como finalidade o seu respeito, suprimindo-se qualquer consideração, ainda que esteja em causa a "persecução dos mais relevantes interesses da justiça criminal", representando uma "intransponível proibição de produção e valoração de prova à custa da invasão daquela área nuclear"[291].

Em suma, torna-se inadmissível qualquer medida que atinja aquela área nuclear da intimidade. Para além de que caso apareçam que as provas recolhidas contendem com aquela área, o uso do programa insidioso deverá ser interrompido.

Todavia, não descuramos a possibilidade da inexistência de um momento prévio de deteção, caso em que não se terá conhecimento do que se poderá vir a encontrar e recolher do sistema informático do suspeito, ou da ativação do *hardware* do mesmo e, assim, começar a ser possível a recolha de dados desse domínio, nos casos em que tal situação ocorra, a proteção da "área nuclear da intimidade" concretizar-se-á na fase de valoração, excluindo aqueles dados. Portanto, impõe-se que o regime não legitime "ações das autoridades judiciárias ou órgãos de polícia criminal que atentem ou invadam a área nuclear da intimidade", sob pena de esse mesmo enunciado normativo ficar ferido inconstitucionalmente[292].

4. Requisitos Orgânicos

Como vimos realçando, a instalação de *malware* será o meio mais gravoso de obtenção de prova, intrusivo e que mais restringe um leque de direitos fundamentais e, portanto, no que aos requisitos orgânico-procedimentais diz respeito, no plano da entidade competente para autorizar a utilização da *malware,* tal competência deve estar reservada ao juiz, conforme artigos 32.º n. 4 e 202.º n.2 da CRP, o princípio da reserva de juiz.

[291] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 167.
[292] CAMPOS, Juliana, A investigação oculta em ambiente digital (…), op. cit. p. 202.

Portanto, o juiz deverá ter o conhecimento sobre o que é o *malware* e sobre as funcionalidades que ele comporta, para poder autorizar. E quando haja necessidade de recorrer a esta medida, o juiz de instrução, através da norma habilitante para uso de *malware*, terá o poder para aferir a admissibilidade do seu uso, adequando ao caso concreto, e desta forma se cumprindo as exigências legais. Assim, incumbe ao juiz de instrução analisar com rigor a restrição de direitos fundamentais, no caso concreto, assegurando "na medida do possível e do exigível, que a intromissão nos direitos consagrados se mantenha sempre mensurável e controlável"[293].

O controlo da legalidade não se confunde com o controlo da oportunidade do juízo realizado pelo Ministério Público, detentor do inquérito, devendo o juiz, de modo autónomo e suficiente, fundamentar a sua autorização, não só delimitando todos os elementos relevantes para uma execução da medida, como também devem os juízes "inteirar-se das circunstâncias de facto e de direito relevantes para a decisão, não se limitando a aderir acriticamente ao juízo formulado pelo MP", quando ele requer este meio de obtenção de prova [294].

Por outro lado, o princípio da reserva de juiz permite ao visado a possibilidade de observar a legitimidade do método e as provas recolhidas através dele. Repare-se que o juiz de instrução não pode ser afastado, dado que o *malware* é um meio de obtenção de prova muito intrusivo; portanto a intervenção do JI deve estender-se ao longo da execução, ou seja, deve ser contínua e "próxima, temporal e materialmente"[295], só desta forma se lhe permitirá o controlo do conteúdo e do tipo de dados informáticos acedidos, o que possibilitará a interrupção, caso se justifique por eventuais exorbitâncias, ou por a sua utilização se tornar desnecessária.

Contudo, sabemos que a prova digital reveste características específicas, tais como, volatilidade, a facilidade de adulteração ou a eliminação da mesma, e assim sendo, nos casos em que seja necessária intervenção célere[296], deve o Ministério Público por despacho autorizar, e posterior validação do juiz. A ausência de autorização do juiz, ou a

[293] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. pp. 168-169.
[294] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 238; ANDRADE, Manuel da Costa «Métodos ocultos de investigação…», op. cit. p. 550.
[295] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 169; A.c. do TC n. 4/06.
[296] Como criminalidade praticada de forma organizada, terrorismo, crimes de homicídio, tráfico de droga, roubo.

falta de fundamentação, no que se refere à suspeita de um crime do catálogo, terá como consequência a ilegalidade da medida e a proibição da valoração do meio de prova.

Em suma, consideramos estes os principais requisitos que deverão constar no regime jurídico deste meio de obtenção de prova.

Conclusões

Na sociedade hodierna, os sistemas informáticos detêm um inigualável valor social e têm um papel central na vida quotidiana de qualquer pessoa.

Este advento das tecnologias de informação veio agilizar os meios de comunicação e potenciar a interação entre as pessoas, alterando por completo o paradigma das relações humanas.

Por outo lado, o fácil acesso à *internet* simplificou a aquisição de bens e serviços, o acesso à informação, e um sem fim de opções, sem que o utilizador tenha que se deslocar. Contudo, esta evolução não apresenta apenas benefícios, pois, se por um lado facilitou a vida dos usuários, por outro veio facilitar o cometimento de ilícitos, com recurso a meios de anonimização, tanto de identidade como de localização dos agentes do crime.

A "crescente sofisticada criminalidade"[297], mais complexa, convoca novos desafios à Justiça, pelo que as autoridades judiciárias e os órgãos de investigação criminal, para atender "às exigências comunitárias"[298] de perseguição penal, veem-se compelidos a dirigir a investigação para o ambiente digital, e a recorrer a novos métodos, ocultos, de obtenção de prova, no âmbito da investigação criminal, concretamente ao *malware*.

O *malware* é um *software* insidioso instalado clandestinamente no sistema informático do suspeito, e destinado à quebra da confidencialidade e integridade dos dados nele contido[299]. Uma vez instalado, ele possibilita a extração e/ou a destruição de dados, permite o acesso a informações, documentos ou, ainda, a monitorização do suspeito em tempo real, sem o seu conhecimento.

Vimos que o uso de *malware* pode ser reconduzido à categoria doutrinal[300] dos métodos ocultos, uma vez que se trata de um *software* instalado de modo oculto no

[297] WEIBLEN, Fabrício Pinto. *Abertura Tecnológica* (…), op. cit.p 19.
[298] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 171.
[299] JR, Aury Lopes; MENDES, Carlos Hélder Carvalho Furtado. "Vírus espião" como meio de investigação: a infiltração por *softwares*. *Revista Consultor Jurídico*. Disponível em https://www.conjur.com.br/2019-jun-07/limite-penal-virus-espiao-meio-investigacao-infiltracao-softwares/ (consultado em 16/03/2024).
[300] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 50.

sistema informático do suspeito, permitindo o acesso a um volume de informações nele incluso, sem que o visado tenha conhecimento.

Enquanto meio de obtenção de prova penal, o *malware* revela uma efetividade sem paralelo, dada a abrangência demostrada na obtenção de material probatório, em contexto de investigações criminais em ambiente digital. De facto, através do *malware,* é possível efetuar a "vigilância na fonte", isto é, aceder aos "dados informáticos *a priori*, da encriptação, ou *a posteriori,* da desencriptação"[301].

Contudo, não podemos olvidar que a introdução do *malware* na investigação criminal suscita conflitos com as finalidades do processo penal e, por outro lado, contende com e restringe um leque de direitos fundamentais, protegidos constitucionalmente, como o direito à autodeterminação informacional, artigos 26º, n.º 1 e 35º da CRP, e o direito à reserva da intimidade da vida privada e familiar, não apenas pelo acesso ao sistema informático, mas também pela recolha de provas externas àquele, quando é, para isso, ativado o *hardware*. Presencia-se, desta forma, uma "devassa daquela área" e a violação de outros direitos fundamentais, nomeadamente do direito à palavra, quando o microfone é ativado, ou do direito à imagem, quando a câmara é ligada, segundo o artigo 26º, n.º 1 da CRP. Vimos também que, com a utilização do *malware,* é possível realizar a vigilância na fonte e, portanto, aceder ao teor desencriptado das comunicações, frustrando as medidas de autoproteção e, consequentemente, ferindo o direito à inviolabilidade das "telecomunicações e nos demais meios de comunicação", conforme artigo 34º, n. º4 da CRP.

Num Estado de Direito, as proibições de prova surgem como garantia do respeito pelos direitos fundamentais e representam uma barreira de "limites intransponíveis" à obtenção de prova a "todo o preço", que se traduzem nos limites da descoberta da verdade material[302]. Elas surgem "como uma das instituições mais marcantes do novo ordenamento processual, erigido a partir dos alicerces sediados diretamente na Constituição de 1976"[303], e são um "dos meios de que se serve a lei para proteger os

[301] *Idem*, p. 45.
[302] ANDRADE, Manuel da Costa, *Sobre as Proibições*…op. cit. p. 123.
[303] *Idem*.

cidadãos contra ingerências abusivas nos seus direitos, no âmbito de uma investigação criminal"[304].

Averiguámos ainda se o *malware* poderia ser introduzido nos meios enganosos de obtenção de prova, isto é, se seria um método proibido de prova, conforme decorre do artigo 126º, n. º2 do CPP, dando lugar a provas nulas, e de acordo com o disposto no artigo 32º, n.º 8 da CRP, que prescreve que são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.

No exemplo analisado, o crime de burla, artigo 217º do CP, vimos que o visado, ao atuar de espontânea vontade e por desconhecimento, pode proceder à instalação deste *software (*por exemplo quando carrega num *link*, num anexo de *email* ou num *site)*, que se apresenta como inofensivo, levando a adotar uma conduta que, erroneamente, o levará à instalação de um programa, comprometendo "a sua liberdade, vontade de decisão"[305]. Aqui concluímos que, apesar de estar comprometida a vontade do suspeito, não podemos afirmar que o envio do *software* malicioso pelos OPC para o sistema informático fosse determinante para a prática do crime e, portanto, o *malware* não se integra nos meios enganosos de obtenção de prova.

Analisámos ainda o princípio *nemo tenetur se ipsum accusare,* que é também um dos limites à descoberta da verdade material, traduzindo-se na garantia do direito de defesa atribuída ao arguido[306], sendo que prescreve o direito à não-autoincriminação. Neste ponto, concluímos que a relação entre o uso investigativo do *malware* e o princípio *nemo tenetur* é de incompatibilidade, se considerarmos que é o próprio visado que, inadvertidamente, procede à instalação do programa insidioso, permitindo assim o acesso às suas próprias declarações, aos dados informáticos em tempo real ou armazenados, ou até mesmo às atividades diretamente autoincriminatórias. Desta forma, estaria o próprio visado em colaboração involuntária com a administração da justiça, tendo em conta que o material recolhido pode ser utilizado contra si no processo penal, ao invés do

[304] SILVA, Germano Marques da. *Curso de Processo Penal* Vol. II, 5.º Edição revista e atualizada, Verbo, 2011. p. 173.
[305] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p. 75.
[306] Com "projeção normativa e prática jurídica dos dispositivos constitucionais atinentes aos da dignidade humana, da liberdade geral da ação ou do direito ao livre desenvolvimento, a liberdade de declaração não é um exclusivo do arguido", ela assiste igualmente a outros sujeitos processuais, nomeadamente à vítima e às testemunhas. ANDRADE, Manuel da Costa, *Sobre as Proibições* (…), op.cit. pp. 126-127.

pretendido. Portanto, a obtenção de declarações autoincriminatórias com recurso a *malware*, no âmbito da investigação criminal, em que o utilizador desconhece que está a ser monitorizado, leva-nos a crer que o princípio do *nemo tenetur* é violado, já que é retirado ao visado o direito ao silêncio, uma vez que ele continua a comunicar de forma espontânea e ingénua, podendo revelar conteúdos que o autoincriminam.

Não obstante, importa ter presente que este princípio não é absoluto, pelo que pode ser restringido, quando a lei assim o determine e sejam verificáveis os pressupostos dos princípios da legalidade e da proporcionalidade, plasmados no artigo 18º, n.º 2 da CRP, o que requer uma análise precisa dos conflitos em causa e, nesse caso, uma vez atendidos os requisitos, poder-se-ia obter prova de conteúdo autoincriminatório com recurso a *malware*.

Averiguámos ainda se o *malware,* enquanto meio de obtenção de prova, encontra base legal no nosso ordenamento. A esse respeito, entendemos que ficou apartada a possibilidade de os artigos 15º, 16º, 17º e 18º todos da LC (obtenção de prova interna ao sistema informático, tanto de dados armazenados, como produzidos em tempo real**)** consubstanciarem alguma base legal para o uso do *malware* na investigação criminal.

Para além da falta de previsão legal, o *malware*, enquanto meio de prova, também não pode ser legitimado ao abrigo de uma qualquer disposição da lei processual penal. Tal se deve a "implicar um elevado grau de intrusão na privacidade do suspeito, com potencial aditivo de perigo inerente ao ataque aos direitos fundamentais", devendo esse uso ser previsto por uma lei expressa, salvo consentimento e informado do visado"[307], pelo que se impõe legitimação da atividade, com precedência de lei formal habilitante,[308]ou decreto-lei exarado pela Assembleia da República, conforme dispõem os artigos 18º, n.º 2 e n.º 3, e também o 165º, alínea b), da Constituição.

Apartámos também a possibilidade do *malware* ser acolhido como meio de obtenção de prova atípico, pois contende com um leque direitos fundamentais, não

[307] *Comentário do código de processo penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos* / org. ALBUQUERQUE. Paulo Pinto de - 5ª ed. atualizada. - Lisboa: Universidade Católica Editora, 2023, pp. 486-487.
[308] RAMALHO, David Silva, *Métodos ocultos* (…), op. cit. p. 216.

respeitando os limites constitucionais impostos no artigo 34º n.º 2 e 4 e no artigo 32º n.º 8 , que resultam do artigo 126º do CPP.

No nosso ordenamento jurídico, tem-se debatido a questão de se o legislador já consagrou devidamente, ou não, a utilização do *malware* em "meios e dispositivos informáticos", no artigo 19 º, n.º 2 da LC, e parte da doutrina tem defendido a sua legitimidade, por se encontrar respaldada por outros meios de prova já legitimados. Por outro lado, também tem sido discutida a questão da compatibilidade deste meio de obtenção de prova com a Constituição nacional.

Quanto a este ponto, vimos que o nosso legislador não foi claro quanto ao significado de "meios e dispositivos informáticos", o que suscita ao intérprete uma dificuldade de densificação normativa quanto a tal conceito.

No nosso entendimento, não acompanhamos a posição da corrente doutrinária que defende que o art. 19º, n.º 2 da LC permite o acesso a "outros meios", para além dos já previstos no nosso ordenamento. Se não vejamos: a expressão "meios e dispositivos informáticos" surge como manifestação ou aceção indeterminada, o que convoca o princípio da determinabilidade dos atos normativos[309], colocando-nos num campo de imprecisão quanto à sua aplicação com a segurança e a certeza exigidas. Pelo que entendemos que o recurso ao *malware* não se encontra legitimado.

Aliado à utilidade deste meio de obtenção de prova, assiste-se a um crescente movimento da sua previsão legal adotado em vários Estados. Por outro lado, o tema da utilização do *malware* tem provocado avultados envolvimento e ponderação, na comunidade jurídica.

É neste enquadramento que se tem invocado a necessidade do uso deste meio oculto no combate à criminalidade organizada, ao terrorismo e à criminalidade económico-financeira, que compõem, atualmente, três das principais ameaças ao Estado de Direito, produzidas com elevado grau de sofisticação que, por sua vez, é conducente a especiais dificuldades investigatórias, que limitam drasticamente os meios abertos de investigação criminal.

[309] CAMPOS, Juliana Filipa Sousa, *O malware* (…), op. cit. p.92.

Na realidade, a "Convenção sobre o Cibercrime celebra mais de duas décadas e a nossa Lei do Cibercrime" começa a dar sinal de necessitar alterações, ao "fim de mais de uma década desde que foi aprovada no nosso ordenamento jurídico"[310]. Portanto, aguarda-se uma intervenção do nosso legislador na consagração legal do uso do *malware*, de forma lisa, transparente e suficientemente densificada, como meio de obtenção de prova em processo penal. Um regime jurídico baseado em vetores bem definidos, na descrição do *malware* como meio de obtenção de prova, cobrindo subsidiariedade, proporcionalidade, catálogo de crimes, grau de suspeita, catálogo de sujeitos, atribuição a autoridade competente, duração, procedimentos a ser observados e informação do sujeito visado depois de terminada a medida.

Atendendo a que a Convenção faculta o uso de "meios processuais e de mecanismos de cooperação internacional, no âmbito dos processos relativos a qualquer crime em que seja necessário recolher prova eletrónica"[311], não se reduzindo apenas a um "Tratado sobre o cibercrime"[312], e tendo em conta que o Direito interno português já acolheu a Convenção sobre o Cibercrime, torna-se determinante a integração de meios de obtenção de prova que permitam às autoridades judiciárias e aos órgãos de polícia criminal levar a bom termo a investigação.

[310] CAMPOS, Juliana, A investigação oculta em ambiente digital …, op. cit. p. 205.
[311] *Idem*.
[312] *Idem*, p. 206.

1 Bibliografia

ALBRECHT, Hans-Jorg. *Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitosAA.VV. Que Futuro Para o direito Processual Penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal.* Coimbra: Coimbra Editora, 2009.

ALBUQUERQUE, Paulo Pinto de. org, *Portugal. Comentário do código de processo penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos.* Lisboa: 5ª Edição atualizada.Universidade Católica Editora, 2023.

ANDRADE, Manuel da Costa. *Bruscamente no Verão Passado. A Reforma do Código de Processo Penal.* Coimbra: Coimbra Editora, 2009.

—. *Métodos ocultos de investigação (Pläydoyer para uma teoria geral). AAVV, Que futuro para o Direito Processual Penal? Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português.* Coimbra: Coimbra Editora, 2009.

—. *Sobre as Proibições de Prova em Processo Penal, 2.ª impressão.* Gestlegal Editora, 2022.

ANTUNES, Maria João. *Direito Processual Penal, 3ª Edição.* Almedina, 2021.

BARATA, Joana Reis. *O regime juridico dos conhecimentos frotuitos em ambiente digítal: contributo da plan view doctrine à luz da legislação portuguesa.In: Novos desfios da prova penal/coord. Paulo Sousa Mendes , Rui Soares Pereira.* Coimbra: Almedina, 2023.

BUEKENHOUT, Inês. "A Investigação criminal." *Desafios presentes e futuros. Investigação Criminal n.º 9, Lisboa,* 2015 de Dezembro.

CAIRES, João Gouveia. "Métodos Ocultos na Criminalidade Económico-Financeira: Entre a (a) tipicidade e a cumulação." *Revista julgar n.º 38*, 2019.

CAMPOS, Juliana Filipa Sousa. "A investigação oculta em ambiente digital." *A utilização de malware. Revista Portuguesa de Ciência Criminal. Ano 32 n.º 1,* Jan-Abril de 2022.

—. *O Malware como Meio de Obtenção de Prova em Processo Penal.* Coimbra: Almedina, 2021.

CORREIA, João Conde. “Prova digital: as leis que temos e as leis que deveriamos ter .” *Revista do Ministério Publico, n.º 139*, setembro de 2014.

GOUVEIA, Jorge Bacelar. *Manual de direito constitucional, vol.II, 6ª edição.* Coimbra: Almedina, 2016.

GRECO, Luís, e GLEIZER, Orlandino. “A infiltrção online no processo penal - Noticia sobre a experiencia alemã.” *Revista Brasileira de Direito Processual Penal, Porto*, s.d.

HARRIS, Ryan. *Arriving at an anti forensics consensus: Examining how to define and control the anti forensics problema. Elsevier.* 2006. https://dfrws.org/presentation/arriving-at-an-anti-forensics-consensus-examining-how-to-define-and-control-the-anti-forensics-problem/ (acedido em 2023).

HENRIQUES, Marco Ribeiro. “Ações Encobertas, para fins de investigação criminal. A dicotomia entre o agente infiltrado e o agente provocador.” *Revista Jurídica UNIGRAN. Dourados, MS | v. 18 | n.º 35*, Jan./Jun. de 2016.

JESUS, Francisco Marcolino de. Os Meios de Obtenção da Prova em Processo Penal-2. a Edição. Leya, 2015. *Os Meios de Obtenção da Prova em Processo Penal-2.ª Edição.* . Lisboa: Leya, 2015.

LOPES, Sónia Raquel da Cruz. “Interceção de comunicações para prova dos crimes de lesões, ameaças, coação, devassa da vida privada e perturbação da paz e do sossego, cometidos por meio diferente do telefone. Revista de Concorrência e Regulação Ano VII, n-º 29.” jan-mar de 2017.

MENDES, Paulo de Sousa. *Lições de Direito Processual Penal.* Coimbra: Almedina, 2020.

MILHEIRO, Tiago Caiado. *Comentário Judiciário do Código de Processo Penal - Tomo II.* Coimbra : Almedina , 2019.

MIRANDA, Jorge, e Rui. MEDEIROS. *Constituição Portuguesa Anotada.* Lisboa: Universidade Católica Editora, 2018.

PELLUCCI, Frederico. *A atuação dos agentes encobertos e infiltrados nos canais abertos e fechados de comunicação em ambiente informático-digital. In: Novos*

desafios da prova penal / coord. Paulo de Sousa Mendes, Rui Soares Pereira. Coimbra : Almedina , 2020.

PEREA, Inmaculada LÓPEZ. BARAJAS. *Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos.* 2017. https://raco.cat/index.php/IDP/article/view/n24-lopez/420451.

PINHEIRO, Alexandre Sousa. *Privacy e protecção de dados pessoais : a construção dogmática do direito à identidade informacional.* Lisboa: AAFDL- Associação Académica da Faculdade de Direito de Lisboa, 2015.

PORTO Editora. *Infopedia. Dicionários Porto Editora.* 2003. https://www.infopedia.pt/artigos/$internet (acedido em 04 de Abril de 2024).

PRADILLO, Juan Carlos Ortiz. "La investigación del delito en la era digital." *Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación. Revista Estudios de Progresso,* 2013.

PRAIA, João de Matos-Cruz. " Proibições de prova em processo penal: algumas particularidades no âmbito da prova por reconhecimento e da reconstituição do facto." *Revista julgar*, Dezembro de 2019.

PROENÇA de Carvalho, F., MORALES García, O., & Álvarez Feijo. *Regulamentação supranacional sobre criminalidade informática e técnicas de transposição: o Direito penal português e espanhol como paradigmas.* 2018.

RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital* . Coimbra : Almedina , 2017.

—. " «O Uso de Malware como Meio de Obtenção de Prova em Processo Penal»." *Revista de Concorrência e Regulação, Ano IV, n.º 16. out- dez.*, 2013.

—. "A Investigação Criminal na Dark WeB." *Revista de Concorrência e Regulação,ano IV, n.º 14/15 abril- set,* 2013.

REAL, Rui Miguel dos Santos. "Meios de Obtenção de Prova e Medidas Cautelares e de Policia." *Trabalhos do 2º Ciclo do 32º Curso do Centro de Estudos Judiciários,* 2019.

RIBEIRO, Gustavo A. M., Pedro Ivo R. V. Cordeiro, e Débora M. , Fumach. “O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro.” *Revista Brasileira de Direito Processual Penal, vol. 8, n. 3,* set- dez de 2022.

RODRIGUES, Anabela Miranda. “A desfesa do arguido: uma garantia constitucuional em perigo no admiravel mundo novo.” *Revista Portuguesa de Ciencia Criminal, ano 12, n.4,* outubro-dezembro de 2002.

RODRIGUES, Benjamim Silva. *Da prova penal: Tomo IV–Da prova-electrónico-digital e da criminalidade informático-digital.* Lisboa: Reis dos Livros,, 2011.

RODRIGUES, Benjamin Silva. *Da Prova Penal: Tomo II - Métodos ocultos de investigação criminal.* Rei dos Livros, 2010.

SCHWALBACH, José Gaspar. *Direito Digital, 2.º Edição.* Coimbra: Almedina, 2021.

SILVA, Germano Marques da. *Curso de Processo Penal.Vol. II, 5.º Edição revista e atualizada.* Verbo, 2011.

—. “«Bufos, Infiltrados, Provocadores E Arrependidos». Direito E Justiça 8 (2), 27-34.1994.” *https://doi.org/10.34632/direitoejustica.1994.10861.*, s.d.

SILVA, Sandra Oliveira e. “Legalidade da prova e provas proibidas.” *Revista Portuguesa de Ciência Criminal, Ano 21, n.º 4, outubro/dezembro ,* 2011.

SOUSA, Paulo Pinto. “ “Ações encobertas: meio enganoso de prova? agente infiltrado e agente provocador. Outras questões.”, Revista do CEJ 2.º semestre, n. º14 .” 2010.

SOUSA, Paulo Pinto de. “Açoes encobertas. Meio enganoso de prova? Agente infiltrado e agente provocador. Outras questões.” *Revista CEJ, 2.º semestre, n.º 14,* 2010.

SOUSA, Susana Aires de. *"Agent provocateur e meios enganosos de prova. Algumas reflexões." Liber Discipulorum para Jorge de Figueiredo Dias.* 2003.

VALENTE, Manuel Monteiro Guedes. “Editorial dossiê Investigação preliminar, meios ocultos e novas tecnologias.” *Revista Brasileira De Direito Processual Penal,* 2017.

—. “Processo Penal, Segurança e Liberdade: uma provocação.” *Revista Brasileira de Direito Processual Penal, Vol I, n.1*, 2015.

—. *Teoria Geral do Direito Policial, 6ªEdição.* Coimbra : Almedina , 2019.

VENÂNCIO, Pedro Dias 2022. “ Lições de Direito do Cibercrime e da tutela penal de dados pessoais.” Coimbra: Editora D'Ideias, 2022.

WEIBLEN, Fabrício Pinto, e Coord. Paulo de Sousa Mendes e Rui Soares Pereira. *Abertura Tecnológica Dos Meios De Obtenção De Prova E O Uso De Software Espião Na Investigação Criminal.* Coimbra: Almedina, 2023.

WOLTER, Jürgen. *O inviolável e o intocável no processo penal. Reflexoes sobre a diginidade humana, proibiçoes de prova, proteção de dados.* São Paulo: Marcial Pons, 2018.

Links consultados

<https://dfrws.org/presentation/arriving-at-an-anti-forensics-consensus-examining-how-to-define-and-control-the-anti-forensics-problem/> (consultado em 26/2/2023)

<https://raco.cat/index.php/IDP/article/view/n24-lopez/420451> (consultado em 12/06/2023).

<https://law.justia.com/cases/federal/district-courts/FSupp2/180/572/2475159/> (consultado em 20/10/2023)

<https://www.numerama.com/politique/23989-le-mouchard-de-la-police-allemande-vise-aussi-skype-gmail-facebook.html> (consultado em 20/10/2023)

http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=200 7-1&nr=38779&pos=11&anz=268 > (consultado em 28/10/2023)

<https://www.bmi.bund.de/EN/topics/security/protection-of-the-constitution/protection-ofthe constitution.html> (consultado em 28/10/2023)

<https://supreme.justia.com/cases/federal/us/277/438/> (consultado em 29/10/2023)

<https://www.justsecurity.org/35136/rule-41-updated-needed/> (consultado em 01/11/2023)

<https://www.tribunalconstitucional.pt/tc/acordaos/20130418.html> (consultado em 5/11/2023)

<https://www.uria.com/documentos/publicaciones/4377/documento/fp02.pdf?id=5591> (consultado em 5/11/2023)

https://www.tribunalconstitucional.pt/tc/conteudo/files/textos/textos0202035.pd (consultado em 10/11/2023)

<https://www.jornaldenegocios.pt/economia/defesa/detalhe/pj-vai-comprar-software-para-extrair-dados-de-telemoveis-a-distancia> (consultado em 11/03/2024)

<https://visao.pt/exameinformatica/noticias-ei/mercados/2021-05-06-pj-sef-gnr-cellebrite-portugal-codigo-azul/> (consultado em 15/03/2024)

<https://www.conjur.com.br/2019-jun-07/limite-penal-virus-espiao-meio-investigacao-infiltracao-softwares/> (consultado em 16/03/2024)

<https://doi.org/10.5281/zenodo.10188525> (consultado em 17/03/2024)

<https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1505&tabela=leis> (consultado em 18/03/2024)

<http://debates.parlamento.pt/catalogo/r3/dar/01/10/04/102/2009-07-10/40?pgs=40-45&org=PLC > (consultado em 21/03/2024)

<https://vlex.es/vid/regulamentacao-supranacional-criminalidade-informatica-741779885> (consultado em 28/03/2024)

<https://www.legifrance.gouv.fr/codes/id/LEGISCTA000023712495/2011-03-16> (consultado em 28/03/2024)

<https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf> (consultado em 28/03/2024)

<https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:PT:PDF> (consultado em 28/03/2024)

<https://www.infopedia.pt/artigos/$internet> (consultado em 02/04/2024)

Acórdãos consultados

Ac. TC n.º 298/19, de 15/5/2019. Relator: Conselheiro Pedro Machete.

Ac. TC. nº418/2013, de 15/07/2013, Relatora Conselheira Catarina Sarmento e Castro.

Ac.TC n.º 364/2006, proc. nº 289/06, de 08/06/2006. Relatora: Conselheira Maria Helena Brito.

A.c. do TC n.º 4/06, processo n.º 665/05, de 03/01/2006. Relator: Conselheiro Mário Torres

Ac. STJ proc. n.º 07P4553, de 20/02/2008. Relator Armindo Monteiro.

Ac. TRE proc. N. º 2871/17.2T8STR.E1, de 14/02/2019. Relator Francisco Matos

Ac. TRL 141/18.8JELSB-A. L1-5, Relator José Adriano

Ac. TRL n.º 40/18.3 JAPDL-A. L1-5, Relator Cid Geraldo

Alemanha

Ac. BverfG, 1 BvR 370, 595/07, de 27 de fevereiro de 2008