De LEGIBUS

IO

Dezembro de 2025

O *MALWARE* ENQUANTO MEIO DE OBTENÇÃO DE PROVA

Malware as a means of obtaining evidence

Gonçalo Amaro Camacho

Revista de Direito
Law Journal

Faculdade de Direito — Universidade Lusófona
https://revistas.ulusofona.pt/index.php/delegibus

O *MALWARE* ENQUANTO MEIO DE OBTENÇÃO DE PROVA

Malware as a means of obtaining evidence

Gonçalo Amaro Camacho*

Sumário: 1. Introdução; 2. Breves noções sobre a prova; 3. A prova digital; 3.1. Enquadramento contextual; 3.2 Características e respetivas dificuldades; 3.3. Princípios processuais aplicáveis; 3.4. Diplomas legais; 4. Os métodos ocultos de investigação criminal; 4.1. Enquadramento geral; 4.2. Requisitos dos métodos ocultos de investigação criminal; 4.3. O agente encoberto no ordenamento jurídico português; 4.3.1. Enquadramento conceptual e legal; 4.3.2. Agente encoberto digital; 5. O *malware* como meio de obtenção de prova; 5.1. Enquadramento conceptual; 5.2. Direito comparado; 5.2.1. Estados Unidos da América; 5.2.2. Alemanha; 5.2.3. Espanha; 5.3. A (in)existência de um regime jurídico na ordem jurídica portuguesa; 5.4. Qual o caminho a seguir?; 6. Conclusão.

Resumo: Os avanços tecnológicos alteraram profundamente a sociedade, sobretudo com a crescente digitalização da vida humana. Esta transição deu origem ao conceito de prova digital, que apresenta características distintas em relação à prova tradicional, como a imaterialidade, volatilidade e suscetibilidade à dissimulação, entre outras. Em paralelo, assiste-se ao surgimento de uma nova criminalidade organizada, que procura tirar máximo proveito deste contexto digital. Neste sentido, emerge a necessidade de métodos ocultos de investigação criminal, mais restritivos dos direitos individuais dos visados, como o uso de *malware* – isto é, a instalação de um *software* malicioso num dispositivo eletrónico do investigado. Diferentemente de países como Alemanha, Estados Unidos e Espanha, Portugal não prevê, pelo menos de forma expressa, esta possibilidade. Assim, a presente investigação visa responder às seguintes questões: deve ser permitido o uso de malware enquanto meio de obtenção de prova? E, em caso afirmativo, quais os moldes jurídicos adequados?

Palavras-chave: prova, prova digital, processo penal, métodos ocultos de investigação criminal, *malware.*

* Formado em Programação e Gestão de Sistemas Informáticos. Licenciado em Direito. Mestre em Ciências Jurídico-Forenses. Explicador em Direito. Email: goncalo.camacho1@hotmail.com.

Abstract: Technological advancements have profoundly transformed society, resulting in the growing digitalization of human activity, often linked to stored digital data or traces left by individuals. This shift has led to the concept of digital evidence, which presents distinct characteristics compared to traditional evidence, such as immateriality, volatility, and susceptibility to dissimulation, among others. Simultaneously, there is an increase in organized crime that seeks to exploit this digital context to its fullest advantage. In this regard, the need for covert criminal investigation methods arises, which are more restrictive of the rights of those under investigation, such as the use of malware—namely, the installation of malicious software on the target's electronic device. Unlike countries like Germany, the United States, and Spain, Portugal does not explicitly allow this possibility. Therefore, this research aims to answer the following questions: should the use of malware as a means of obtaining evidence be permitted? And if so, under what legal framework?

Keywords: evidence, digital evidence, criminal procedure, covert criminal investigation methods, malware.

1. Introdução

O avanço civilizacional trilha um caminho onde a progressiva transição do mundo físico para o ambiente tecnológico é uma realidade incontornável. Basta atendermos à forma como as pessoas atualmente levam a cabo o seu dia-a-dia, onde as suas comunicações, trabalhos e transações estão fortemente dependentes de meios tecnológicos que possuem ao seu dispor.

A par disto, assistimos, por um lado, à readaptação dos fenómenos criminais tradicionais e, por outro, ao surgimento de novas formas de criminalidade como a pornografia infantil e ataques informáticos. Este contexto fez com que os métodos tradicionais de obtenção de prova se tornassem insuficientes para um combate efetivo deste novo panorama.

O legislador, reconhecendo este problema, criou a denominada Lei do Cibercrime a 15 de setembro de 2009. No entanto, a realidade prática tem apontado no sentido de ainda existir um longo percurso na criação de mecanismos de investigação criminal eficazes para conseguir resolver estas problemáticas.

Aqui chegados, tendo em conta a crescente digitalização conjugada com as especificidades da prova digital, torna-se imperativo perceber se faz sentido

a utilização de meios como o *malware*, ou seja, um vírus colocado no sistema informático do visado, para a obtenção de prova. Ora, este confronto torna-se particularmente problemático especialmente quando nos deparamos com a versatilidade de funções que este meio consegue assumir e, consequentemente, violar os direitos individuais do investigado.

Deste modo, com o presente estudo pretendemos realizar uma análise doutrinal das obras portuguesas mais importantes que refletiram sobre o assunto, bem como olhar brevemente para o sistema jurídico de três países que utilizam este instituto jurídico, de modo a avaliar se o Direito português deve legitimar a utilização do *malware* enquanto meio de obtenção de prova, tendo em conta, por um lado, as dificuldades de obtenção de prova no espaço digital e, por outro, as restrições dos direitos do visado.

2. Breves noções sobre a prova

Considerando o objeto de estudo, a presente investigação tem como ponto de partida a prova. A etimologia da palavra "prova" (do latim *probare*) remete-nos para a ideia de testar ou demonstrar que algo possui determinado valor. Desta noção, depreendemos que o objetivo da prova é criar um estado de certeza ou convicção perante um terceiro, apresentando-se como o meio pelo qual a verdade sobre o que ocorreu em determinado contexto chega a seu conhecimento.

No âmbito processual penal, de acordo com Maria João Antunes[1], uma das funções deste processo é a realização da justiça e a descoberta da verdade material. Em torno desta temática encontramos um assunto estruturante: a prova.

Se é certo que um dos objetivos principais deste ramo processual é o da descoberta de toda a factualidade em torno de um crime, para que tal aconteça torna-se necessário conseguir arranjar elementos que provem que o crime ocorreu naqueles termos, sendo isto o que efetivamente se compatibiliza com a ideia atual que temos de realização de justiça.

Ora, o artigo 124.º do Código de Processo Penal (CPP) estabelece que: "1- Constituem objecto da prova *todos os factos* juridicamente relevantes para

1 Maria João Antunes, *Direito Processual Penal*, 3.ª edição, (Coimbra: Almedina, 2022), 18.

a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis" [itálico nosso].

Nessa exata medida, vale a pena sublinhar que este conjunto de factos levados a juízo são geralmente obtidos através dos meios de obtenção de prova, sendo estes mecanismos que visam a obtenção de elementos que servirão para demonstrar a realidade de determinado conjunto fático[2].

3. A prova digital

3.1. Enquadramento contextual

Hodiernamente, os avanços tecnológicos trouxeram consigo inegáveis vantagens na forma como as pessoas comunicam, se deslocam, adquirem produtos, obtêm informações, entre outros, muitas vezes à simples distância de um "clique"[3]. No entanto, não demorou até que estas facilidades começassem a ser alvo de uma visão oportunista para levar a cabo práticas maliciosas[4]. Deste tipo de condutas surgiu a necessidade de o legislador regulamentar estas áreas através, nomeadamente, dos denominados "crimes informáticos".

Vulgarmente, é utilizada a noção de cibercrime como todo o tipo de atividades criminosas levadas a cabo por meios informáticos. No entanto, esta delineação apresenta um problema claro, que é o facto de nesta aceção também incidirem todos os crimes em que o computador ou telemóvel foi um instrumento lateral na questão em análise, como por exemplo nos crimes de injúria, difamação ou coação. Assim, consideramos que a

2 Francisco Marcolino de Jesus, *Os Meios de Obtenção da Prova em Processo Penal* (Coimbra: Almedina, 2015), 139.

3 Neste tocante, Pedro Freitas aponta até para uma "dependência informática" onde é impensável viver sem aparelhos informáticos na sociedade atual. José Pedro Freitas, *Os meios de obtenção de prova digital na investigação criminal: o regime jurídico dos serviços de correio eletrónico e de mensagens curtas,* (Braga: Novacausa, 2020), 53-55.

4 Armando Dias Ramos, "Crimes praticados com recurso à Internet na sociedade de risco - Contributo para o estudo de dois cibercrimes" (Relatório de mestrado científico em Ciências Jurídico-Criminais, Universidade de Lisboa, Faculdade de Direito, 2009), 40.

definição mais precisa de cibercrime é a seguinte: "o tipo de criminalidade onde o elemento digital ou informático surge como componente que integra o tipo legal"[5].

Indubitavelmente, ao longo dos últimos anos temos assistido a um aumento constante dos crimes informáticos que, ao que tudo indica, não parece abrandar num futuro próximo. Como podemos verificar, de acordo com o relatório anual de segurança interna de 2023[6], entre os anos 2013 e 2023, verificou-se um aumento de aproximadamente 700%, tendo o registo anual de crimes transitado de 359 para 2512 infrações.

Não obstante, destacamos novamente, o panorama atual dita uma realidade onde não apenas o aumento da cibercriminalidade é factual, como também grande parte dos restantes crimes praticados têm algum tipo de conexão com o digital. O que queremos dizer com isto é que grande parte das comunicações, interações, movimentações da nossa sociedade deixam de alguma forma uma pegada digital que é crucial em qualquer investigação criminal nos dias de hoje.

Aqui chegados, importa relacionar o assinalado com a prova digital, que, nas palavras de Dias Ramos, esta entende-se como a "informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e completa"[7].

3.2. Características e respetivas dificuldades

Por estarmos diante de uma realidade diversa dos meios de prova tradicionais que encontramos, por exemplo, num crime de furto ou de homicídio, as características inerentes a esta prova também são bastante distintas.

5 José Ricardo Marques Branco, "Prova digital. Os meios de obtenção de prova digital e a restrição de direitos do arguido", (Dissertação de Mestrado em Ciências Jurídico-Forenses, Faculdade de Direito da Universidade de Coimbra, 2021), 16.

6 "Relatório Anual de Segurança Interna de 2023", acesso em 1/08/2024, https://www.portugal.gov.pt/

7 Armando Dias Ramos, *A Prova Digital em Processo Penal*, 1.ª edição, (Lisboa: Chiado Editora, 2014), 86.

Em primeiro lugar, temos uma *natureza remota,* em que o crime pode ser praticado de qualquer ponto do mundo com um qualquer dispositivo com conexão à *internet*, o que resulta numa enorme volatilidade quanto à movimentação do criminoso. A par disto, existe ainda acesso bastante simplificado aos meios necessários para a prática do crime em questão, o que desencadeia a rápida aquisição e posterior destruição dos equipamentos utilizados.

De seguida, assinalamos que estamos perante uma prova *imaterial*, por vezes *codificada*[8], o que exige conhecimentos técnicos especializados para conseguir obter a prova em causa sem que esta seja comprometida ou alterada. Para tal, basta pensar no cenário em que determinado documento essencial para a investigação se encontra não apenas criptografado, mas também numa *cloud*[9] apenas acessível através de determinado *proxy*[10].

Além do mais, muitas vezes verificamos um caráter *temporário* ou de fácil *alterabilidade*[11], uma vez que a natureza da prova em questão pode ter já pré-definida a sua destruição ou mutação, ou ainda ser suscetível de uma alteração posterior dos dados inicialmente estabelecidos, o que frequentemente impossibilita a devida investigação criminal em tempo útil. A título de exemplo, trazemos à colação dois cenários bastante elucidativos dados por Dias Meireles[12]: A, em conversações através de um *chat* digital, confessa a B determinado crime, porém logo em seguida elimina todas as mensagens, impedindo também a B o posterior acesso às mesmas; ou ainda, C, no decurso de um

8 Para uma análise mais aprofundada deste assunto, *vide* Juliana Filipa Sousa Campos, *O Malware como Meio de Obtenção da Prova em Processo Penal* (Coimbra: Edições Almedina, 2021), 41-48; De salientar o comentário de Paul Ohm, que sobre este ponto nos refere que: "The government's need to use malware to investigate crime is almost always connected to a target's successful use of encryption. A criminal target or suspect who communicates without encryption can usually be tracked without resort to malware." Paul Ohm, "The Investigative Dynamics of the Use of Malware by Law Enforcement", in *William & Mary Bill of Rights Journal*, vol. 26, Issue 2 (December 2017), 317.

9 Sistema informático de armazenamento de dados que permite o acesso dos mesmos de forma remota.

10 Um servidor intermediário entre o utilizador e determinado serviço a que se pretende aceder.

11 Fazemos nota do referido por Barreto Furtado: "Atualmente, a eliminação, alteração e ocultação desses elementos não exigem dos seus proprietários um concreto know-how tecnológico, na medida em que existem programas informáticos disponíveis para download que efetivamente exercem essas tarefas de modificação e alteração da metadata." Rafael João Barreto Furtado, "Os limites da utilização do malware" (Dissertação de Mestrado em Direito e Prática Jurídica – Especialidade em Direito Penal, Faculdade de Direito da Universidade de Lisboa, 2020), 33; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3.ª ed. (Amsterdam, Elsevier, 2011), 26.

12 Ana Isa Dias Meireles, *A Prova Digital no Processo Judicial* (Coimbra: Almedina, 2023), 105.

processo judicial junta aos autos um documento *pdf.* essencial para as suas alegações, não sem antes, claro, alterar alguns dados a seu favor.

Outro ponto importante é o facto de a prova digital ser, muitas vezes, circunstancial, dificultando a responsabilização de um indivíduo por atividades realizadas através de um dos seus dispositivos[13]. Pode sempre ser alegado que outra pessoa, de forma legítima ou não, teve acesso ao dispositivo e realizou a atividade analisada, sendo necessário articular esta prova com outras que permitam demonstrar, de forma mais segura, quem efetivamente cometeu o crime em causa.

Uma última característica prende-se com a natureza *transnacional* deste delito, que implica uma necessidade de os órgãos de investigação terem a capacidade de investigar em vastos espaços geográficos, o que nem sempre é possível, uma vez que existem países com os quais não existem protocolos ou legislação regulamentadora de cooperação internacional. Além disso, acrescem dificuldades especialmente quando estamos perante infratores que têm o mínimo de conhecimentos informáticos e que, aquando da prática dos delitos, utilizam ferramentas como VPN[14] ou um sistema *onion routing*[15].

Aqui chegados, é fácil compreender a complexidade da produção de prova neste contexto, muitas vezes inviabilizada por diversos obstáculos: porque surge já criptografada ou adulterada, porque a investigação colide com países que recusam colaborar, ou ainda por outras razões.

3.3. Princípios processuais aplicáveis

Tendo por base as particularidades supra enunciadas, além da aplicação dos princípios gerais do processo penal, sempre que se proceda à obtenção de prova digital será necessário ter em conta um conjunto de princípios específicos.

13 Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3.ª ed. (Amsterdam, Elsevier, 2011), 26.

14 Virtual Private Network – Uma conexão segura e criptografada que serve de intermediário entre o utilizador e os servidores a que acede.

15 A expressão "roteamento em cebola" pretende retratar precisamente as várias camadas existentes na cebola. Transpondo esta ideia para um sistema de redes de computação, um dado antes de chegar ao destino passa por diversos servidores para dificultar a capacidade de identificarmos a origem e o conteúdo da mensagem.

Em primeiro lugar, tendo em conta a fácil alterabilidade, um dos princípios fundamentais é o da *não alteração da prova eletrónico-digital* no ato de recolha, armazenamento e de tratamento forense, que representa um cuidado acrescido para o agente que trabalha na prova de não contaminar os dados da mesma de qualquer forma, o que pode aqui significar a necessidade de conhecimentos técnicos adequados.

Em seguida, temos dois princípios que poderão ser correlacionados, *o princípio da documentação* de todas as fases – acesso, recolha, armazenamento, preservação ou apresentação – e o *princípio da pessoalidade do controlo da cadeia de custódia*. Neste tocante, por um lado o investigador está sujeito a uma descrição detalhada de todas as etapas relacionadas com a produção de prova e, por outro, recai sobre o mesmo uma responsabilidade pessoal sobre toda a prova produzida[16].

Não obstante, devido à complexidade destes processos, não raras vezes surge e necessidade de várias entidades intervirem, de modo que existe a necessidade da aplicação do *princípio da responsabilidade repartida* dos vários intervenientes, que estabelece a necessidade de todos respeitarem estritamente o conjunto de princípios forenses digitais.

Por fim, destacamos o *princípio da especialização ou qualificação do pessoal de investigação* que passa por dotar os mesmos com os conhecimentos técnico-científicos necessários para lidar com esta prova[17].

3.4. Diplomas legais

Atualmente são três os diplomas que regulam estas matérias: o CPP, nos artigos 187.º a 189.º, a Lei n.º 32/2008, de 17 de junho e a Lei n.º

16 Neste tocante, Benjamim Silva Rodrigues refere-nos que este princípio muitas vezes remete-nos para uma proibição de terceiros poderem aceder a objetos alvo da perícia digital. Benjamim Silva Rodrigues, *Da Prova Penal, Tomo IV – Da Prova Eletrónico-Digital e da Criminalidade Informático-Digital*, 1ª edição, (Lisboa: Rei dos livros, 2011), 45-46.

17 Pela pertinência desta dualidade dialogante, destacamos o comentário de Costa Marques que nos refere que "invariavelmente, os técnicos não têm formação jurídica adequada e os juristas têm dificuldade em entender as nuances técnicas dos equipamentos e da informação neles armazenada". Pedro Penha Leitão da Costa Marques, "Informática Forense: Recolha e preservação da prova digital", (Dissertação para obtenção do grau de Mestre em Segurança em Sistemas de Informação, Universidade Católica Portuguesa, Faculdade de Engenharia, 2013), 12.

109/2009, de 15 de setembro, mais conhecida por Lei do Cibercrime (LC). Aqui chegados, destacamos a ausência de uma lei uniformizadora, algo que leva vários autores[18] a apontarem para a existência de um regime que necessita urgentemente de ser reformado, pois apresenta áreas de regulação comuns entre as diversas leis, não resultando claro qual deverá ser o diploma aplicável.

O CPP, nas normas suprarreferidas, estabelece o regime jurídico das escutas telefónicas. No artigo 187.º encontram-se plasmados os termos da sua admissibilidade no processo, no artigo 188.º todas as formalidades necessárias que devem ser cumpridas caso se venha a utilizar este meio de prova e, por fim, no artigo 189.º temos o que se pode denominar de "cláusula de extensão", que faz com que o presente regime se aplique "às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática". Este último ponto abona, efetivamente, a favor das críticas supra enunciadas, uma vez que resulta daqui uma cláusula excessivamente abrangente que colide com disposições de outros diplomas.

Relativamente à Lei n.º 32/2008, de 17 de junho, a mesma possui um conjunto de disposições que têm como objetivo regular a conservação e transmissão dos dados de tráfego e localização, e os dados relevantes para a identificação do utilizador.

Por fim, temos a LC, onde entre os artigos 3.º e 11.º encontramos um conjunto de normas penais, vulgarmente designadas de "crimes informáticos", ao passo que do artigo 12.º até ao 19.º encontramos um conjunto de disposições processuais, tendo em vista a obtenção de prova em ambiente digital. Por outro lado, as disposições entre os artigos 20.º ao 26.º estabelecem regras sobre a cooperação internacional.

18 Branco, "Prova digital", 21-22 e Alberto Gil Lima Cancela, "A prova digital: os meios de obtenção de prova na lei do cibercrime" (Dissertação de Mestrado na Área de Especialização em Ciências Jurídico- Forenses, Universidade de Coimbra, 2016), 25.

4. Os métodos ocultos de investigação criminal

4.1. Enquadramento geral

A utilização de métodos ocultos de investigação consiste no emprego de meios enganosos ou dissimulados com o objetivo de comprometer, de alguma forma, o investigado que, não se apercebendo deste meio, continua a proceder à atividade criminosa.

Podemos considerar como métodos ocultos de investigação as intromissões nas telecomunicações, os agentes encobertos, a observação oculta, a gravação de imagens ou de palavras com câmaras ou microfones, o controlo por sistemas de geolocalização, entre outros.

Aqui chegados, tendo como premissa as dificuldades já suscitadas pela prova no ambiente digital, torna-se cada vez mais dominante o entendimento de que é necessário a utilização daqueles métodos neste espaço[19-20.]

Por outro lado, não deixa de ser notória a colisão com vários direitos individuais, dos quais destacamos a reserva da intimidade da vida privada, direito à autodeterminação informacional, o direito à imagem e à palavra, a inviolabilidade do domicílio e, também com diversas garantias processuais, designadamente, o direito de não se autoincriminar, o contraditório, a presunção de inocência e lealdade processual.

Em Portugal, assistimos a uma diversificação de diplomas que preveem a possibilidade de utilização de métodos ocultos. Alguns destes regimes poderão ser encontrados no CPP, na LC, na Lei Nº 5/2002, de 11 de janeiro e na Lei Nº 101/2001, de 25 de agosto.

Apesar de reconhecermos a existência de uma diversidade de métodos ocultos de investigação criminal, a nossa análise centrar-se-á no regime

19 Neste sentido: Maria Ana Barroso de Silveira, "Da problemática da investigação criminal em ambiente digital, em especial sobre a possibilidade de utilização do malware como meio oculto de obtenção de prova", (Dissertação de Mestrado, Faculdade de Direito da Universidade Católica de Lisboa, 2016), 13; Furtado, "Os Limites*", 10;* David Silva Ramalho, *Os métodos ocultos de investigação criminal em ambiente digital* (Coimbra: Almedina, 2017), 202-206;

20 Destacamos ainda Manuel Costa Andrade, que nos refere que a utilização destes meios se massificou ao longo das últimas duas décadas motivadas, por um lado, por uma ideologia de combate ao terrorismo dos Estados Unidos da América e, por outro, pelos sucessivos avanços tecnológicos. Manuel da Costa Andrade, *"Bruscamente no Verão Passado", a reforma do Código Penal – Observações críticas sobre uma Lei que podia e devia ter sido diferente* (Coimbra: Coimbra Editora, 2009), 105.

jurídico das ações encobertas (RJAE), com foco especial na figura do agente encoberto digital. Esta escolha justifica-se pela especificidade deste regime em conjugar a necessidade de apuramento da verdade material com a proteção dos direitos fundamentais do investigado. Dada a natureza altamente invasiva deste tipo de atuação, que, ao contrário de outros métodos ocultos de investigação, permite um acompanhamento contínuo, em tempo real e na proximidade da esfera digital do suspeito, à semelhança do *malware*. Deste modo, deparamo-nos assim com mecanismos que assumem contornos de uma verdadeira busca domiciliária virtual.

4.2. Requisitos dos métodos ocultos de investigação criminal

Não obstante o conjunto diversificado de métodos ocultos existentes, é possível encontrar uma unidade comum de requisitos que necessitam estar presentes para que a utilização daquele meio seja legítima[21].

Em primeiro lugar, a restrição de qualquer direito fundamental terá necessariamente de passar pelo crivo do princípio da proporcionalidade, previsto no artigo 18.º, n.º 2 da Constituição da República Portuguesa (CRP), exigindo-se um balanceamento concreto entre os direitos que se pretendem restringir e os direitos que se pretendem salvaguardar. Este princípio pode ser decomposto em três vertentes: o princípio da adequação, que determina que a medida adotada deve ser apta a assegurar o fim visado; o princípio da necessidade, que impõe aos poderes públicos o dever de optar pela medida adequada menos onerosa para o cidadão; e o princípio da proporcionalidade em sentido estrito, que exige que o sacrifício dos direitos restringidos não seja excessivo face às vantagens obtidas com a medida.

Depois encontramos a reserva de lei, que nos remete para a necessidade de existência de uma lei específica que preveja restrição do direito fundamental

21 Alertamos para o facto de uma das críticas da doutrina neste tocante ser a falta de uniformização destes meios, encontram-se os mesmos dispersos entre Código do Processo Penal e outros diplomas extravagantes. *Ibidem*, 108-109.

em causa, onde se estabeleça os pressupostos, configuração, extensão e os respetivos destinatários, estando aqui vedada qualquer tipo de "restrições em branco"[22].

Costa Andrade[23] aponta ainda para a necessidade de um catálogo de infrações que legitime a utilização daquele meio, bem como em concreto se terá de verificar a suspeita fundada da ocorrência do mesmo.

Por outro lado, temos ainda o requisito da *subsidiariedade* do método utilizado, optando, *prima facie*, pela utilização de métodos não ocultos e, caso se verifique que a utilização destes não é suficiente, se proceda à utilização dos meios ocultos. Em seguida, teremos ainda de dar preferência aos métodos ocultos que sejam menos lesivos, e apenas após verificado que estes não se configuram como eficazes, se poderá passar a outros mais gravosos[24]. Assim, torna-se nítida uma correlação entre o princípio em apreço e o subprincípio da necessidade anteriormente analisado.

Finalmente, será necessária a *reserva do juiz*, estando aqui assente a ideia de que sempre que se torne necessário recorrer a medida que restrinja direitos fundamentais a decisão terá de passar pelo juiz, em consonância com o disposto no artigo 32.º, n.º 4 e 202.º, n.º 2 da CRP.

4.3. O agente encoberto no ordenamento jurídico português

4.3.1. Enquadramento conceptual e legal

Podemos entender como agente encoberto determinado indivíduo que, ocultando a sua verdadeira qualidade ou identidade[25], entra numa esfera onde

22 Duarte Alberto Rodrigo Nunes, *O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada*, (Coimbra: Gestlegal, 2019), 283.

23 Costa Andrade, *"Bruscamente no Verão Passado"*, 114.

24 Destacamos a denominação conferida por Benjamim Silva Rodrigues, que se reporta a esta questão como subsidiariedade em "cascata". Benjamim Silva Rodrigues, *Da prova penal- Tomo II- Bruscamente... A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal* (Lisboa: Rei dos Livros, 2010), 57.

25 Frederico Pellucci, "A atuação dos agentes encobertos e infiltrados nos canais abertos e fechados de comunicação em Ambiente informático-Digital", *in Novos Desafios da Prova Penal*, (Coimbra, Almedina, 2020), 258.

são praticados comportamentos ilícitos com o intuito de posteriormente os vir a reportar às autoridades competentes.

O regime jurídico em análise torna-se particularmente restritivo para com os sujeitos envolvidos, uma vez que o agente em questão atua naquele meio durante um período considerável e, em virtude disso, estabelece relações de confiança e amizade com os infratores, havendo lugar a um natural relaxamento quanto à prática dos vários delitos na presença do agente[26].

Ora, o surgimento do RJAE nasce com a Proposta de Lei N.º 79/VIII/2[27], apresentado pelo então ministro da Justiça António Costa, tendo em vista o combate à criminalidade grave e organizada, utilizando como principal argumento a necessidade de dar uma resposta mais adequada à criminalidade organizada transnacional[28]. Daqui resultou a aprovação do referido diploma.

É no seu artigo 1.º, n.º 1, que encontramos o seu âmbito de aplicação, sendo tal para "fins de prevenção e investigação criminal". Já no n.º 2 desse artigo temos a definição de ação encoberta: "Consideram-se acções encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade."

Não obstante, o artigo 3.º estabelece os requisitos que permitem o uso deste instituto jurídico, ao dispor que: "As acções encobertas devem ser adequadas aos fins de prevenção e repressão criminais identificados em concreto, nomeadamente a descoberta de material probatório, e proporcionais quer àquelas finalidades quer à gravidade do crime em investigação." Este contexto naturalmente suscita um dos mais importantes princípios do direito constitucional, o princípio da proporcionalidade (artigo 18.º, n.º 2, da Constituição

26 Assinalamos neste ponto a distinção feita pela doutrina sobre as ações encobertas *light cover* e *deep cover*, cuja diferença reside na duração do tempo que o agente esteve encoberto. As primeiras duram menos de seis mesesÇPPP, ao passo que as segundas têm de ultrapassar esse período. Ana Rita Almeida Guedes, "O agente encoberto digital enquanto método oculto de obtenção de prova" (Dissertação de Mestrado em Ciências Jurídico-Forenses, Faculdade de Direito da Universidade de Coimbra, 2021), 13; António José da Silva Catana, "A natureza jurídica da ação do agente infiltrado digital", (Dissertação de mestrado em Ciências Policiais, Instituto Superior de Polícia e Segurança Interna, 2018), 37.

27 "Proposta de Lei n.º 79/VIII/2", acesso em 10 de agosto de 2024, https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=18560.

28 "Reunião plenária de 22 de junho de 2001, publicada no Diário da Assembleia da República n.º 99/2001", acesso em 10 de agosto de 2024, https://debates.parlamento.pt/~.

da República Portuguesa), obrigando-nos a fazer uma cuidadosa valoração entre os objetivos que pretendemos alcançar com aquele meio, por um lado, e os direitos, liberdades e garantias que poderão ser restringidos[29].

4.3.2. Agente encoberto digital

A figura do agente encoberto digital foi uma inovação trazida pela *internet*, que transpôs a possibilidade de utilizar esta figura no espaço digital. Em países como os Estados Unidos da América, que possuem uma das redes de investigação criminal mais desenvolvidas tecnicamente, atualmente é bastante comum a utilização deste método para combater criminalidade relacionada com o tráfico de droga, pornografia infantil e pedofilia, especialmente em espaços como a *Deep Web*[30], devido à natural dificuldade de prova que os atos aqui praticados acarretam.

Na ordem jurídica portuguesa temos o artigo 19.º da LC que estabelece as ações encobertas no espaço digital. Todavia, esta norma, ao invés de estabelecer um regime próprio, tendo em conta as especificidades do meio digital, faz antes uma remissão para o RJAE, caso estejamos perante um dos crimes indicados nesse artigo.

Naturalmente, este feito não passou despercebido pela doutrina[31], que aponta constantemente para a necessidade de uma devida adaptação deste regime ao meio digital, uma vez que existem diversas diferenças em relação ao meio físico. Apresentando alguns exemplos, no meio digital o agente pode assumir de uma forma muito mais facilitada diferentes identidades e perfis em simultâneo: num momento poderá aparentar ser um pedófilo e, no momento

29 Destacamos o facto de esta valoração ser sempre realizada através dos subprincípios deste princípio geral, designadamente: princípio da adequação; princípio da necessidade; princípio da proporcionalidade em sentido estrito. Armando Dias Ramos, *O agente encoberto digital: Meios especiais e técnicos de investigação criminal*, (Coimbra: Almedina, 2022), 37.

30 Este termo reporta-se às camadas da Internet inacessíveis através dos motores de busca tradicionais, que atualmente constituem cerca de 90% da internet. As mesmas apenas podem ser acedidas através de *software e*specífico que permita esta ligação, como por exemplo o Tor Browser.

31 Ana Rita Almeida Guedes, "O agente encoberto digital enquanto método oculto de obtenção de prova" (Dissertação de Mestrado em Ciências Jurídico-Forenses, Faculdade de Direito da Universidade de Coimbra, 2021), 35; David Silva Ramalho, *Métodos ocultos de investigação criminal em ambiente digital* (Coimbra: Almedina, 2019), 284.

seguinte, um menor de idade. Depois, no meio físico existe uma muito maior dificuldade de recolha de prova, uma vez que o agente nem sempre tem acesso aos elementos necessários para consegui-lo, por estar fisicamente na presença dos criminosos e ter de continuamente "representar um papel". Já no meio digital, isto não sucede, visto que o agente, enquanto atua, pode estar a gravar tudo o que sucede no *chat*, *website*, ou sistema a que está a aceder sem qualquer risco para o próprio. Além disso, o conjunto de ferramentas técnicas que o investigador dispõe no ambiente digital possibilita-lhe, sem grande risco, o aprofundar da investigação durante o seu decurso. Nesta ótica, o meio digital permite ir além do que está a ser apresentado pelo investigado de uma forma muito mais fácil, comparativamente ao meio físico.

5. O *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA

5.1. Enquadramento conceptual

A terminologia de *malware* é a junção de duas palavras, *malicious* (malicioso) e *software* (programa). Assim, estamos perante um programa informático que foi concebido para se infiltrar noutro sistema com o intuito de executar determinadas tarefas. Estas podem ir desde a monitorização do outro sistema em tempo real, consulta ou destruição de dados, dar instruções ao computador infetado, para se transmitir para outros sistemas. No fundo, existe aqui uma particularidade: a versatilidade de formas que o *malware* pode assumir, sendo-lhe possível controlar totalmente outro sistema como se o indivíduo estivesse fisicamente a utilizar o mesmo.

Aqui chegados, destacamos o facto de este *software* ser utilizado de forma sub-reptícia[32], instalando-se sem a perceção do utilizador e aí permanecendo perante o seu total desconhecimento, podendo levar a cabo um conjunto multifacetado de ações. Este contexto faz com este meio seja fortemente restritivo de diversos direitos individuais do visado, tais como o direito à

32 Destacamos a terminologia referida por Mónica Barroso Costa, que ao longo da sua dissertação se reporta à utilização do *malware* como um "tipo de agente infiltrado virtual". Mónica Barroso Costa, "O malware como o agente infiltrado na criminalidade organizada", (Dissertação de Doutoramento em Ciências Jurídico-Criminais, Faculdade de Direito da Universidade de lisboa, 2023), 147.

reserva da intimidade da vida privada (artigo 26.º, n.º 1 da CRP), o direito à autodeterminação informacional (artigo 35.º da CRP), direito à imagem e à palavra (artigo 26.º, n.º 1 da CRP), direito à inviolabilidade do domicílio (artigo 34.º da CRP), direito ao sigilo e proteção das comunicações (artigo 34.º, n.º 4, da CRP).

A título exemplificativo, temos inúmeras categorias onde estes são agrupados consoante as suas funcionalidades, entre as quais destacamos: cavalos de troia; *logic bombs*; *keylogger*.

Um cavalo de troia é um *malware* que se disfarça de um ficheiro legítimo para enganar o utilizador a instalá-lo. Uma vez no sistema, este abre portas a um acesso remoto por parte do atacante com o intuito de se apropriar de dados.

O *logic bomb* é uma secção de código malicioso programada para ser executada em condições específicas, com uma data, hora ou acontecimento. Este tipo de *malware* permanece latente até que a condição programada seja cumprida, momento em que desencadeia a sua ação, que pode incluir a eliminação de ficheiros, danos no sistema ou envio de dados para terceiros.

Um *keylogger* é um *software* que regista secretamente as teclas pressionadas pelo utilizador no teclado. A sua principal função é capturar informações sensíveis, como credenciais de *login*, números de cartão de crédito e mensagens privadas.

5.2. Direito Comparado

5.2.1 Estados Unidos da América

Muito embora os indícios da utilização do *malware* como método de investigação criminal pelas autoridades competentes dos Estados Unidos da América remontem aos inícios dos anos 90, o primeiro caso relatado foi o de *United States v. Nicodemo S. Scarfo and Frank Paolercio*[33], a 15 de janeiro de 1999.

33 U.S. District Court for the District of New Jersey, *No*. 00-4313 de 26 de dezembro de 2001, acesso em 30 de outubro de 2024, https://law.justia.com/cases/new-york/court-of-appeals/2013/123.html.

Neste caso, o Federal Bureau of Investigation *(FBI)* desenvolveu um *keylogger*, que guardava o registo das teclas pressionadas no sistema informático pelo investigado, Nicodemo Scarfo, o então chefe da Máfia Americana (*Cosa Nostra*), com o intuito de ter acesso a um ficheiro altamente encriptado no seu computador, cuja palavra-passe apenas era conhecida por este. A utilização deste meio de obtenção de prova foi aceite em tribunal.

Dois anos depois, ocorreu a célebre situação que resultou na criação do *software* denominado de "*Magic Lantern*", bastante semelhante ao *malware* utilizado no caso Scarfo, mas com a particularidade de se tornar desnecessário o acesso físico ao computador de destino.

Quanto a legislação norteadora destas ações, temos duas, a quarta emenda[34], que se refere à proteção contra buscas e apreensões arbitrárias, isto é, sem que haja um motivo razoável ou mandado judicial que se baseie em causa provável (*probable cause)*, e ainda a *rule 41 – Search and seizure in federal rules of criminal procedure*, que estabelece os moldes em que devem ser feitas buscas e apreensões, em particular no ponto *6*[35].

5.2.2 Alemanha

A Alemanha, através do Tribunal Constitucional Federal Alemão (BVerfG), no dia 27 de fevereiro de 2008, levou a cabo um marco histórico, ao reconhecer um novo direito fundamental: o direito à integridade e confidencialidade dos sistemas informáticos. A decisão surgiu em resposta a uma lei

34 Sobre se a utilização do *malware* enquanto meio de obtenção de prova deve ser considerada uma search, em consonância com a quarta emenda, Paul Ohm conclui favoravelmente, embora, conforme frise, não se trata de uma questão unânime na doutrina. *Vide* Paul Ohm, "The Investigative Dynamics of the Use of Malware by Law Enforcement", 327-329.

35 "Um juiz magistrado com autoridade em qualquer distrito onde possam ter ocorrido atividades relacionadas com um crime tem autoridade para emitir um mandado para usar o acesso remoto para pesquisar meios de armazenamento eletrónicos e para apreender ou copiar informações armazenadas eletronicamente localizadas dentro ou fora desse distrito se:

(A) o distrito onde os meios de comunicação ou informações estão localizados foi ocultado por meios tecnológicos; ou

(B) estivermos perante uma violação do título 18 do código dos Estados Unidos, dentro da secção 1030(a)(5), onde os meios de comunicação são computadores protegidos que foram danificados sem autorização e estão localizados em cinco ou mais distritos." [tradução nossa].

da Renânia do Norte-Vestfália que permitia a vigilância secreta de computadores pessoais através de *software* espião para prevenir crimes.

O Tribunal considerou que os sistemas informáticos contêm informações sensíveis sobre a vida privada, exigindo proteção contra acessos não autorizados. Estabeleceu-se que apenas ameaças graves, como a segurança nacional ou a vida humana, poderiam justificar tal interferência, desde que sujeita a supervisão judicial.

Este direito fundamental garante que os dados armazenados em sistemas informáticos sejam protegidos contra acessos não autorizados, assegurando a confidencialidade e a integridade dos mesmos, de modo a preservar a privacidade dos cidadãos no contexto digital.

Atualmente, a Alemanha, no seu processo penal (*Strafprozeßordnung* – StPO), estabelece, no parágrafo 100b, uma autorização para realizar buscas *online* (*Online Durchsuchung*), possibilitando a utilização de *software* informático para obter dados armazenados ou produzidos em tempo real pelo visado.

Na subsecção n.º 1 do artigo em questão, encontramos que os meios técnicos podem ser utilizados para aceder aos sistemas informáticos, sem o conhecimento do visado, para a obtenção de dados. Este contexto obedece ao princípio da necessidade, só podendo este meio ser utilizado caso a investigação dos factos seja dificilmente obtida ou impossibilitada mediante outros meios investigatórios.

Já na subsecção n.º 2, estabelece um catálogo dos crimes onde se poderá proceder à utilização destes meios, designadamente, que atentem contra a autodeterminação sexual, falsificação de dinheiro, terrorismo, homicídio culposo, organizações criminosas.

Por outro lado, a subsecção n.º 3 circunscreve a medida à possibilidade de apenas ser utilizada contra o acusado, todavia caso o mesmo faça uso de sistema informático de terceiro para praticar o crime, ou se durante a pesquisa se chegue à conclusão de que a intervenção apenas no sistema informático do visado não é suficiente para procedência da investigação, a lei permite estender esta medida a outras pessoas que não o acusado.

5.2.3 Espanha

Em Espanha, o *malware* como meio de obtenção de prova está regulado na *Ley de Enjuiciamiento Criminal*, no artigo 588.º *septies* (a) a (c). Assim, a utilização deste instrumento exige não só o cumprimento dos critérios legais de ponderação (reconhecidos pela doutrina e pela jurisprudência, de forma geral), mas também a consideração de diversos parâmetros avaliados pelo juiz competente no momento de autorizar a medida.

Para o avanço deste procedimento, a investigação tem de estar necessariamente relacionada com o seguinte catálogo de crimes: delitos cometidos no seio de organizações criminosas; delitos de terrorismo; delitos cometidos contra menores ou pessoas com a capacidade modificada judicialmente; delitos contra a Constituição, de traição e relativos à segurança nacional; e delitos cometidos através de instrumentos informáticos ou de qualquer outra tecnologia de informação ou comunicação ou serviço de comunicação.

Por outro lado, o n.º 2 do mesmo preceito determina que a decisão judicial tem de especificar: os sistemas ou dispositivos informáticos que serão objeto da medida; o alcance da medida, a forma como se procederá o acesso e apreensão dos dados ou ficheiros informáticos relevantes para a causa e o *software* que irá executar o controlo da informação; os agentes autorizados para a medida; a autorização, no caso, para a realização e conservação de cópias dos dados informáticos; as medidas precisas para a preservação da integridade dos dados informáticos, assim como para a inacessibilidade ou supressão dos referidos dados do sistema informático a que se tenha acedido.

Por fim, realçamos que o artigo 588.º *septies* (c) estabelece o limite temporal da utilização da medida num prazo máximo de um mês, possivelmente renovável por períodos da mesma duração, até o máximo de três meses.

5.3. A (in)existência de um regime jurídico na ordem jurídica portuguesa

Direcionemos agora o foco para a discussão em torno da possibilidade da existência de algum suporte normativo no nosso ordenamento jurídico, que

permita proceder à utilização do *malware* enquanto meio de obtenção de prova.

Conde Correia[36-37] admite a possibilidade da utilização deste meio através de uma interpretação do artigo 19.º, n.º 2 da LC[38], uma vez que esta abre a possibilidade de realizar ações encobertas com recurso a meios e dispositivos informáticos, sendo certo que este mecanismo só deve ser utilizado nos casos excecionais em que seja possível a realização da ação encoberta.

Já Pinto Albuquerque, refere-nos de forma clara que "A busca *online* foi agora consagrada pelo novo artigo 15.º da Lei n.º 109/2009, de 15/9, que prevê a 'pesquisa em sistema informático' (...)"[39].

Em sentido contrário temos visões como a de Castanheira Neves[40-41], que exclui a hipótese da LC admitir esta possibilidade nos artigos 15.º e da 16.º do diploma, uma vez que não foi aqui consagrada a possibilidade de recolha de dados sem o consentimento do visado.

No nosso entendimento, tendemos a ser favoráveis a uma tese que defende a inexistência de consagração legal do *malware* na LC. Pois, atendendo às particularidades inerentes do *malware*, que lhe permitem não apenas monitorizar em tempo real o visado e as respetivas comunicações a que procede, como também aceder a dados armazenados no sistema informático, não se nos afigura como razoável um encaixe forçoso em nenhum dos artigos suprarreferidos, uma vez que uma interpretação literal dos mesmos não torna possível o encaixe de todas as características inerentes deste meio. Além do mais, uma interpretação do artigo 19.º, n.º 2 que inclua este meio parece-nos

36 João Conde Correia, "Prova digital: as leis que temos e a lei que devíamos ter" in *Revista do Ministério Público*, n.º 139, ano 35, (2014), 43.

37 Marcolino Francisco Jesus também se mostra favorável a este entendimento, embora não refira qual a consagração legal deste mecanismo. Francisco Marcolino de Jesus, *Os Meios de Obtenção da Prova em Processo Penal*, 2.ª edição, (Coimbra: Almedina, 2015), 246.

38 Neste sentido: Silva Ramalho, *Os métodos ocultos de investigação criminal em ambiente digital*, 338.

39 Paulo Pinto de Albuquerque, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4.ª edição, (Lisboa: Universidade Católica Editora, 2018), 502.

40 Rita Castanheira Neves, *As ingerências nas comunicações electrónicas em processo penal*, (Coimbra: Coimbra editora, 2011), 284.

41 No mesmo sentido: Paulo Dá Mesquita, *Processo Penal, Prova e Sistema Judiciário* (Coimbra: Coimbra Editora, 2010), 115.

simplesmente demasiado extensiva desviando-se daquilo que fora a teleologia da lei, bem como violadora do requisito da *reserva de lei* que se já no agente encoberto digital se encontra beliscado, quanto à utilização do *malware*, dúvidas não restam quanto à sua violação, uma vez que este é um meio ainda mais gravoso, pois o visado não possui o mínimo grau de suspeita de que esteja a ser monitorizado por alguém.

5.4. Qual o caminho a seguir?

Sedimentada a base da discussão que nos pareceu ser mais relevante, cumpre-nos agora perceber qual deve ser a resposta por parte da nossa ordem jurídica para a utilização do *malware* enquanto meio de obtenção de prova.

Comecemos por frisar alguns direitos que são fortemente restringidos aquando da utilização deste meio. O direito à reserva da intimidade da vida privada, consagrado no artigo 26.º, n.º 1 da CRP, pressupõe que cada um tenha a possibilidade de desenvolver um conjunto de atos na sua esfera privada sem a ingerência de terceiros. Neste ponto, a jurisprudência alemã desenvolve este conceito em três esferas[42]: esfera da vida íntima, que corresponde a um domínio pessoal inviolável; esfera da vida privada, cujos factos são partilhados apenas com um grupo restrito de pessoas; esfera da vida pública que já envolve os factos suscetíveis de serem conhecidos por qualquer pessoa.

Adicionalmente, face ao avanço da era digital, revela-se pertinente o reconhecimento como direito fundamental do direito à confidencialidade e integridade dos sistemas informáticos, também delineado pela jurisprudência alemã. Este direito deve ser enquadrado à luz da dignidade da pessoa humana (artigo 2.º da CRP) e do livre desenvolvimento da personalidade (artigo 26.º, n.º 1 da CRP), garantindo a proteção da privacidade dos dados criados, processados e/ou armazenados nos dispositivos informáticos dos cidadãos.

Por outro lado, o artigo 35.º da CRP consagra o direito à autodeterminação informacional, que consiste no direito de cada individuo controlar os dados disponíveis a seu respeito. Ademais, não poderíamos deixar de referir o direito à palavra e à imagem (artigo 26.º, n. º 1 da CRP) que, grosso modo,

42 Ac. STJ, de 20-06-2012, P.º 417/10.2TTVNF.P1.S1, acesso em 1/12/2024, www.dgsi.pt.

consistem na ideia de que o indivíduo titular do direito controlar quem pode ter acesso às suas conversações e quaisquer retratos que se reportem à sua pessoa.

Ora, tendo em conta as especificidades do *malware*, que conseguem com relativa facilidade monitorizar em tempo real as palavras, imagens, dados armazenados em sistema e localização do dispositivo, surge aqui a possibilidade de fazer um acompanhamento multifacetado do visado quando este se encontra mais relaxado e, consequentemente, apanhá-lo desprevenido não apenas a praticar crimes, mas também a levar a cabo as tarefas da sua vida sem qualquer substrato ilícito.

Deste modo, o recurso ao *malware* como meio de obtenção de prova apresenta um potencial significativo para reproduzir, de forma fidedigna, a vida física e psicológica do visado, assumindo-se como um verdadeiro diário íntimo digital[43] que regista todos os passos deste. Tal caraterística torna evidente a suscetibilidade deste método colidir com os direitos fundamentais anteriormente referidos.

A esta visão poder-se-á opor o argumento de que vivemos numa era marcada pela banalização dos dados pessoais, em que grande parte das informações privadas se encontra acessível ao público através de diversas plataformas, como as redes sociais. Todavia, esta realidade reforça a necessidade de conferir uma proteção acrescida ao núcleo essencial da reserva da vida privada, que surge como o direito mais suscetível de ser afetado por este meio de obtenção de prova. Apesar da crescente tendência para a partilha voluntária de dados pessoais, a importância de preservar a esfera íntima da vida privada, onde se inserem os aspetos que a pessoa não pretende divulgar, assume hoje maior relevância que nunca, pois torna-se talvez o último resquício de privacidade que a pessoa deliberadamente não pretende ver partilhado.

Assim, a utilização deste método deve ser interditada nos casos em que se preveja uma afetação da esfera íntima da vida pessoal do visado. No entanto,

43 Washington Trindade da Silva Junior, "A utilização de malware em investigações criminais em face do estabelecido pelos direitos fundamentais", (Dissertação de Mestrado em Direito na especialidade de Direito Público, Faculdade de Direito da Universidade Nova de Lisboa, 2021), 50; Maria Ana Barroso de Moura da Silveira, "Da problemática da investigação criminal em ambiente digital – em especial, sobre a possibilidade de utilização do malware como meio oculto de obtenção de prova" (Dissertação de Mestrado em Direito, Universidade Católica Portuguesa, Faculdade de Direito – Escola de Lisboa, 2016), 42.

para evitar que tal limitação se transforme numa estratégia para ocultar provas incriminatórias, admite-se uma exceção à regra geral: o recurso ao *malware* poderá ser permitido quando houver fundadas razões para crer que a informação probatória se encontra misturada com dados de natureza íntima, desde que, num momento posterior, se proceda à eliminação de todos os elementos irrelevantes para o processo.

Por outro lado, reparamos também a restrição de diversas garantias processuais como é o caso do princípio da presunção de inocência (artigo 32.º, n.º 2 da CRP) que dita que consideremos a pessoa suspeita como inocente até ao trânsito em julgado da decisão, sendo certo que um dos corolários deste princípio é precisamente o direito que a pessoa tem de não se autoincriminar. Além disso, temos também o princípio do contraditório (artigo 32.º, n.º 5 da CRP), ou seja, a possibilidade do visado poder em igualdade de armas proceder à contraprova, e também o princípio da lealdade processual que vincula todos os sujeitos e intervenientes processuais à aquisição e produção de prova de forma leal para com os restantes no processo.

Novamente, observamos um conjunto de normas consolidadas, neste caso em termos processuais, que são fortemente restringidas com a utilização do *malware*. A constante monitorização do presumido inocente, enquanto este, sem qualquer conhecimento, continua a contribuir com elementos essenciais para produção de prova contra si, pode de facto ser interpretada como um meio desleal que, por sua vez, acarreta um fator surpresa que apenas lhe confere a possibilidade de resposta no processo num momento muito posterior ao desejado.

No reverso da medalha, encontramos um conjunto de questões que nos apontam para os perigos da crescente digitalização societária. Onde se verifica uma criminalidade organizada cada vez mais complexa, que não conhece fronteiras físicas, enquanto utiliza um conjunto de equipamentos, denominados de medidas antiforenses[44], que lhe permite desenvolver as suas práticas de forma anónima, criptografada[45] e sem deixar necessariamente

44 David Silva Ramalho, "O uso de malware como meio de obtenção de prova em Processo Penal", *in Revista de Concorrência e Regulação,* Ano 4, n.º 16 (Outubro-Dezembro 2013): 208-212.

45 Especificamente quanto a esta questão, Sousa Campos refere-nos que "face à emergência da encriptação de dados, (...), a investigação criminal encontra-se dificultada ou impossibilitada". Campos, *O Malware como Meio de Obtenção da Prova em Processo Penal*, 54.

um rasto para a investigação criminal dada a efemeridade e mutabilidade dos dados digitais.

A par disto, recordamos as características e princípios rígidos aplicáveis à prova digital que dificultam a obtenção de provas no espaço digital, ao requererem uma documentação detalhada de todas as etapas da investigação criminal, onde um simples erro técnico pode comprometer toda uma investigação. Além do mais, tendo em conta a tecnicidade da prova em análise, esta análise não está ao alcance de qualquer investigador, uma vez que requer conhecimentos específicos para lidar com a mesma.

Aqui chegados, conjugados os conflitos em apreço, pugnamos pela utilização do *malware* enquanto meio de obtenção de prova. A crescente transição para um mundo mais dependente de mecanismos tecnológicos é uma realidade inevitável cabendo ao Direito estar apto para conseguir responder a este novo fenómeno, e a utilização do *malware* representa precisamente isto.

Não obstante, não nos podemos olvidar da capacidade extrema para restringir direitos individuais deste meio, de modo que a ordem jurídica terá necessariamente de adotar um regime que tenha em consideração diversos aspetos formais e materiais[46].

Em primeiro lugar, considerando o carácter altamente restritivo deste meio, destaca-se a imprescindibilidade da intervenção judicial obrigatória, competindo ao juiz autorizar a sua utilização, fixar o prazo máximo de aplicação até três meses num determinado dispositivo informático e determinar a eventual renovação, se devidamente justificada.

Como ponto de partida, cabe à figura judicial fazer desde logo uma confrontação da factualidade concreta com o princípio da proporcionalidade[47], à luz dos seus três subprincípios. Deste modo, uma vez verificado que este meio é apto a assegurar o fim visado, torna-se imperativo perceber se, em correlação com o princípio da subsidiariedade de fora para dentro, não existe qualquer outro meio de investigação criminal

46 Neste sentido: Juliana Filipa Sousa Campos, "A investigação oculta em ambiente digital", *in Revista Portuguesa de Ciência Criminal*, ano 32 n.º 1, (2022): 192-193.

47 Fabio Nicolicchia, "Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova", *in Diritto penale contemporaneo,* 8 gennaio 2018, 16, acesso em 05/03/2025, https://archiviodpc.dirittopenaleuomo.org/.

menos oneroso para o visado, que também seja adequado. Finalmente, a utilização desta medida deve assentar numa avaliação casuística entre os direitos sacrificados e os benefícios obtidos, devendo o juiz rejeitar a sua validação caso verifique uma desproporção entre os ganhos e os prejuízos causados[48].

Tal como se verifica nas ordens jurídicas espanhola e alemã, será necessário estabelecer um catálogo de crimes graves, cuja verificação no caso concreto justifique a utilização deste meio. Além disso, deve ser definido que este só poderá ser utilizado nas fases de inquérito e instrução, impedindo, assim, o seu uso de forma preventiva[49].

De facto, este mecanismo assume uma versatilidade tremenda nas funções que pode vir a assumir, de modo que um mandado judicial neste sentido, à semelhança do que se verifica em Espanha, deve definir qual o objeto visado pela investigação, permitindo uma perceção sobre que tipo de direitos podem ser restringidos, para que as equipas de investigação criminal estejam limitadas na escolha do vírus que podem utilizar. Tendo em conta este dado, as equipas decidem qual o meio mais adequado, se um *keylogger o*u cavalo de

48 Pela elevada pertinência da análise efetuada por Lorena Bachmaier Winter sobre este ponto, reforçando a necessidade de existir um catálogo para a aplicação deste meio: "En general, cuando se trate de delitos de criminalidad organizada transnacional y terrorismo, o delitos cometidos contra menores y personas incapaces, la restricción del derecho a la privacidad estará legitimada, incluso a través del registro remoto de equipos informáticos. Ahora bien, cuando estamos ante delitos cometidos a través de sistemas informáticos la aplicación del principio de proporcionalidad ya no resulta tan fácil, sobre todo porque el perjuicio que esos delitos causan a la sociedad no sempre resulta tan evidente. En esos casos, en los que la pena prevista para el delito no es elevada, la gravedad del delito no justifica per se el sacrificio de los derechos fundamentales de los indivíduos". Lorena Bachmaier Winter, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *in Boletín del Ministerio de Justicia, Año* LXXI, Núm. 2195, 2017, 23, acesso em 05/03/2025, https://revistas.mjusticia.gob.es/.

49 Divergimos da opinião de Lydie Jorge Batista, que defende a utilização preventiva do *malware* em casos de crimes cometidos por organizações terroristas, de terrorismo e de terrorismo internacional. Consideramos que o panorama jurídico atual em Portugal não justifica a admissibilidade deste regime, uma vez que esses crimes são, atualmente, uma questão residual. Além disso, acabaria por criar uma desarmonia normativa com o regime das escutas telefónicas, sendo este um método oculto de investigação criminal menos gravoso e que não pode ser utilizado de forma preventiva. Lydie Jorge Batista, "O Malware como Meio de Obtenção de Prova em Processo Penal", (Dissertação de Mestrado em Ciências Jurídico-Forenses, Faculdade de Direito, Universidade de Lisboa, 2018), 136; Também no sentido perfilhado por nós temos a ordem jurídica espanhola, conforme destaca Lorena Bachmaier Winter: "El sistema español, a diferencia de otros ordenamientos, no permite utilizar medidas de investigación restrictivas de derechos fundamentales con fines preventivos o prospectivos.". Sendo isto proibido expressamente pelo artigo 588 bis (a) (2) do Código Processual Penal espanhol. Lorena Bachmaier Winter, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", 8.

troia, pretendendo com isto a não existência de uma investigação que vá para além do fim definido. Por exemplo, pretendia-se o acesso a um dado armazenado no sistema do visado, porém, como foi concedido livremente o uso do *malware*, foi também utilizado para monitorizar em tempo real a localização e ativado o microfone do mesmo, obtendo informações que claramente apresentam um desvio ao que era inicialmente pretendido.

Adicionalmente, deve ser estabelecido que a prova obtida através deste meio só é válida apenas contra o visado, não podendo ser utilizada para fundamentar a responsabilização penal de outras pessoas, bem como não devem ser registadas conversações que envolvam comunicações entre o arguido e o seu defensor, ou entre o arguido e pessoas legalmente habilitadas a recusar o depoimento com fundamento no segredo profissional.

Assim, este mecanismo funciona como um garante de que as equipas de investigação criminal, antes de solicitarem ao juiz a autorização para utilizar este método, reflitam cuidadosamente sobre a identidade do visado e em que moldes pretendem utilizar este método. Nessa medida, restringir da prova a este indivíduo específico procura evitar que métodos ocultos de obtenção de prova sejam aplicados de forma indiscriminada, assegurando que a investigação seja direcionada de forma precisa. Não obstante, conforme estabelecido no regime alemão, seria importante deixar uma ressalva neste regime. Se, durante a investigação, se concluir que a intervenção exclusiva no sistema informático do visado não é suficiente para o prosseguimento da investigação, a lei deve permitir a extensão dessa medida a outras pessoas que não o acusado.

Para além disso, o indivíduo responsável pela utilização deste método deve elaborar um relatório semanal, documentando todas as operações realizadas, bem como os dados recolhidos, que deverá ser enviado ao Ministério Público, que terá um prazo de 24 horas para se pronunciar. Caso se verifique a conformidade legal das operações deverá o mesmo enviar o relatório para o Juiz de Instrução criminal, também sujeito a um prazo de 24 horas, de modo a garantir um controlo judicial da questão.

6. Conclusão

O mundo atual acompanhou um crescimento exponencial da tecnologia onde a vida das pessoas passou a estar profundamente interligada aos meios tecnológicos. Com isto, não apenas os fenómenos criminais começaram a transitar do mundo físico para o mundo virtual, conforme verificamos através de dados estatísticos que apontam para o crescimento gradual da criminalidade informática, como também parte da criminalidade tradicional utiliza, de alguma forma, um meio tecnológico.

Este contexto torna necessária a análise da prova digital e dos princípios processuais que lhe são aplicáveis, os quais a distinguem significativamente da prova tradicional. Com efeito, a prova digital apresenta particularidades que dificultam a sua obtenção, podendo gerar cenários de impunidade que, associados ao crescimento contínuo desta criminalidade, revelam a urgência de uma resposta por parte do Direito.

Nesta senda, surgem os métodos ocultos de investigação criminal, que constituem meios mais gravosos para os direitos individuais, dada a falta de perceção do visado quanto à sua utilização. Por isso, a sua aplicação depende do cumprimento de diversos requisitos.

Centremos agora a atenção na possibilidade de utilizar *malware* como meio de obtenção de prova no espaço digital. Embora se trate de um tema ainda recente entre nós, outras ordens jurídicas recorrem a este instrumento há mais de duas décadas para responder aos desafios da criminalidade digital.

Relativamente ao ordenamento jurídico português, começamos por indagar sobre a discussão doutrinária referente à possibilidade de existência de um regime normativo que permita proceder à utilização deste meio. Concluímos pela negativa, convictos de que ainda não existe qualquer suporte legal que tenha em conta as especificidades fortemente restritivas de direitos que o *malware* comporta.

Consideramos, no entanto, que é de extrema importância que o Direito acompanhe a realidade, adotando o *malware* como meio de obtenção de prova, de forma a superar as dificuldades inerentes à prova digital. A questão essencial reside na definição dos contornos para a sua integração no ordenamento jurídico. Propomos, assim, um conjunto de critérios

gerais, que incluem a reserva de lei, a limitação da medida a um catálogo restrito de crimes, a necessidade de autorização judicial para a sua aplicação por um período temporal determinado, a identificação precisa do objeto alvo da investigação, a delimitação dos direitos suscetíveis de restrição e a ponderação da medida à luz dos princípios da proporcionalidade e da subsidiariedade.

Data de Submissão: Novembro de 2024
Data de Aceitação: Outubro de 2025
DOI: https://doi.org/10.60543/dlb.vi10.9805