UNIVERSIDADE D
COIMBRA

Andreia Filipa Santos Duarte

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

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses, orientada pela Professora Doutora Sónia Mariza Florêncio Fidalgo e apresentada à Faculdade de Direito da Universidade de Coimbra

Julho de 2022

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

Andreia Filipa Santos Duarte

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

MALWARE AS A MEANS OF OBTAINING EVIDENCE IN CRIMINAL PROCEEDINGS

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Ciências Jurídico-Forenses (conducente ao grau de Mestre), orientada pela Professora Doutora Sónia Mariza Florêncio Fidalgo

Coimbra, 2022

AGRADECIMENTOS

Ao longo da elaboração da presente dissertação, foram várias as pessoas que me apoiaram e, acima de tudo, motivaram, garantindo assim que todo o meu esforço e dedicação culminassem neste trabalho.

Desde logo, começo por agradecer à Professora Doutora Sónia Fidalgo, pela orientação e disponibilidade, assim como pelos conselhos e críticas construtivas. Foi nas suas aulas que aprofundei o meu gosto pela temática da prova no processo penal, nomeadamente a prova digital, o que contribuiu bastante para a escolha deste tema e elaboração desta dissertação.

Quero também agradecer àqueles que são os meus pilares em todos os momentos. Aos meus pais, por serem o meu maior e melhor exemplo a seguir, por me darem força e apoio incondicionais, em todas as etapas, dia após dia. Aos meus avós e aos meus tios, por acreditarem sempre em mim e no meu potencial.

Por fim, agradeço aos meus amigos. Na impossibilidade de enumerar todos, destaco aquelas que foram o meu maior suporte ao longo deste caminho: Sofia, Catarina, Mafalda e Miranda, o meu mais sincero obrigada.

RESUMO

Com o desenvolvimento tecnológico, surgiram formas de criminalidade mais complexas e sofisticadas que vieram tornar a obtenção de prova bastante mais difícil. Assim, a investigação criminal deparou-se com desafios que pareciam ser insuperáveis com o recurso aos tradicionais métodos, pensados essencialmente para a realidade física e não digital. Com efeito, torna-se necessário dotar as autoridades competentes de novos meios e técnicas capazes de fazer face a estes entraves, garantindo assim que tais entidades também acompanham o progresso tecnológico e estão munidas dos instrumentos necessários para garantir a eficácia da ação penal.

Neste panorama, o *malware* passou a ser visto como uma ferramenta muito útil e um potencial meio de obtenção de prova no âmbito do processo penal. Tratando-se de um método oculto de investigação, não podemos ignorar a permanente tensão que este método convoca, designadamente entre a descoberta da verdade material e a proteção dos direitos fundamentais. Assim, impõe-se que seja encontrado o ponto de compatibilização entre estes interesses, tarefa esta que deve caber ao legislador aquando da sua regulação.

Neste sentido, temos assistido à consagração deste método de obtenção de prova em vários ordenamentos jurídicos, quer na Europa, quer nos EUA. De facto, os EUA são um país onde a utilização do *malware* é bastante recorrente, reunindo uma grande coletânea de casos e destacando-se como pioneiro de operações de enorme sucesso.

Por sua vez, em Portugal, a utilização deste método pelas entidades responsáveis pela investigação é, aparentemente, desconhecida e a doutrina divide-se quanto à questão de saber se este já está ou não consagrado no nosso ordenamento jurídico, nomeadamente na Lei do Cibercrime. A verdade é que, tendo em conta as especificidades do *malware*, não nos parece que o recurso ao mesmo possa ser legitimado com base noutros preceitos; pelo contrário, esta eventual consagração reclama uma lei expressa, clara e determinada que discipline, autonomamente, o seu regime jurídico.

PALAVRAS-CHAVE

Prova; prova digital; processo penal; investigação criminal; métodos ocultos; *malware*; direitos fundamentais; conflito entre as finalidades do processo penal; ANOM; UFED

ABSTRACT

With technological development, more complex and sophisticated forms of crime have emerged that have made obtaining evidence far more difficult. Thus, criminal investigation has been faced with challenges that seemed insurmountable with the use of traditional methods, designed essentially for the physical and not digital reality. In fact, it became necessary to provide the competent authorities with new means and techniques capable of dealing with these obstacles, thus ensuring that such entities also keep up with technological progress and are equipped with the necessary tools to ensure the effectiveness of criminal prosecution.

In this scenario, malware has come to be seen as a very useful tool and a potential means of obtaining evidence in criminal proceedings. Since it is a covert method of investigation, we cannot ignore the permanent tension that this method involves, namely between the discovery of the material truth and the protection of fundamental rights. Therefore, it is necessary to find the point of compatibility between these interests, a task that should be up to the legislator when regulating it.

In this sense, we have witnessed the establishment of this method of obtaining evidence in several legal systems, both in Europe and in the USA. In fact, the US is a country where the use of malware is quite recurrent, gathering a large collection of cases and standing out as a pioneer of extremely successful operations.

In turn, in Portugal, the use of this method by the entities responsible for the investigation is apparently unknown and the doctrine is divided as to whether or not it is already enshrined in our legal system, namely in the Cybercrime Law. The truth is that, taking into account the specificities of malware, it does not seem to us that its use can be legitimized based on other precepts; on the contrary, this possible consecration requires an express, clear and determined law that autonomously regulates its legal regime.

KEYWORDS

Evidence; digital evidence; criminal procedure; criminal investigation; covert methods; malware; fundamental rights; conflict of purposes of criminal procedure; ANOM; UFED

SIGLAS E ABREVIATURAS

AFP – *Australian Federal Police*

AJ – Autoridade(s) Judiciária(s)

art., arts. – artigo, artigos

cf. – confira, confronte

cit. – citado, citada

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

EUA – Estados Unidos da América

FBI – *Federal Bureau of Investigation*

FRCP – *Federal Rules of Criminal Procedure*

GNR – Guarda Nacional Republicana

LAE – Lei das Ações Encobertas

LC – Lei do Cibercrime

MP – Ministério Público

n.º, n.ºs – número, números

p., pp. – página, páginas

OPC – Órgão(s) de Polícia Criminal

PJ – Polícia Judiciária

SEF – Serviço de Estrangeiros e Fronteiras

ss. – seguintes

UFED – *Universal Forensic Extraction Device*

ÍNDICE

INTRODUÇÃO

Atualmente, vivemos numa sociedade marcada pela era digital e pelos sucessivos avanços tecnológicos, que exigem que as pessoas e as instituições se adaptem rapidamente a novas técnicas e novos métodos.

Neste sentido, de há uns anos a esta parte, torna-se fundamental que também a investigação criminal acompanhe esta evolução, de modo a garantir a sua eficácia. Assim, a utilização de novos meios de obtenção de prova, designadamente ao nível da prova digital, revela-se muito importante, na medida em que também os agentes da prática de crimes recorrem, cada vez mais, a estas novas tecnologias como *modus operandi*, o que pode dificultar ou até impossibilitar a recolha de prova através dos métodos tradicionais.

Deste modo, alguns países têm permitido a utilização, pelas entidades responsáveis pela investigação criminal, de *softwares* maliciosos[1] enquanto meio de obtenção de prova, como forma de ultrapassar os obstáculos colocados no acesso aos sistemas informáticos fruto do enorme desenvolvimento tecnológico a que temos assistido.

Não obstante a evidente necessidade e utilidade de recorrer a este tipo de métodos ocultos, é imprescindível refletir sobre os conflitos emergentes entre as finalidades do processo penal neste campo, nomeadamente entre a descoberta da verdade material e a realização da justiça, por um lado, e a proteção dos direitos fundamentais dos cidadãos (designadamente, do arguido), por outro. De facto, no âmbito da prova, em geral, e dos seus meios de obtenção, em particular, a tensão entre estas duas finalidades é permanente e levantam-se inúmeras dificuldades quando se pretende obter a sua concordância prática[2].

Apesar de, em Portugal, esta prática não estar (ainda) regulada, tem particular interesse discutir sobre a sua eventual consagração legal e os termos em que esta poderá ser admitida, sendo de máxima importância chegar a um consenso e propor a adoção de um regime jurídico, com requisitos específicos e dentro de pressupostos apertados, que permita harmonizar as referidas finalidades do processo penal.

[1] Doravante designados simplesmente por "*malware*".
[2] ANTUNES, Maria João, *Direito Processual Penal*. 3.ª Edição, Coimbra: Almedina, 2021, p. 18

Assim, na nossa análise, iremos refletir sobre a utilização de *malware* como meio de obtenção de prova em processo penal. Primeiramente, exige-se uma contextualização do tema na atualidade, bem como uma explicação da sua utilidade e relevância prática no âmbito da investigação criminal.

Num segundo momento, procederemos a um enquadramento deste meio de obtenção de prova no processo penal, nomeadamente no que diz respeito à sua integração nos métodos ocultos de investigação e à acima referida tensão entre as finalidades do processo.

Depois de uma breve referência a alguns ordenamentos jurídicos estrangeiros, procederemos a uma exposição relativa ao uso de *malware* no ordenamento jurídico americano – como fio condutor para o capítulo seguinte, bem como faremos uma análise à legislação portuguesa, concluindo pela ausência de regulação expressa deste meio de obtenção de prova no nosso ordenamento jurídico, culminando na apresentação de um conjunto de requisitos para que a utilização de *malware* possa vir a ser constitucional e legalmente admissível[3] em Portugal.

Por sua vez, numa vertente mais prática, será apresentada uma operação de sucesso, levada a cabo pelas autoridades americanas e australianas, que, graças à utilização deste inovador meio de obtenção de prova, permitiu desmantelar redes criminosas e grupos organizados por todo o mundo, culminando na detenção e prisão de centenas de pessoas e na apreensão de toneladas de material e estupefacientes. Por fim, e numa perspetiva de reflexão, colocaremos a hipótese (ou não) de ser levada a cabo uma operação idêntica em Portugal.

[3] CAMPOS, Juliana, *O malware como meio de obtenção da prova em processo penal*, Coimbra: Almedina, 2021, p. 29

CAPÍTULO I

O *MALWARE*: A UTILIZAÇÃO COMO MEIO DE OBTENÇÃO DE PROVA E O ENQUADRAMENTO NO PROCESSO PENAL

1. Contextualização na atualidade

Nos últimos anos, os Estados têm procurado munir-se de instrumentos que lhes permitam penetrar no ambiente digital do indivíduo aquando da investigação criminal[4]. Esta é uma realidade inegável, na medida em que, atualmente, a prova digital constitui o cerne da generalidade dos processos penais[5].

A verdade é que vivemos numa sociedade marcada pela era digital[6] e assistimos diariamente a sucessivos avanços tecnológicos nos mais diversos domínios da nossa vida[7], o que, inevitavelmente, conduz a que cada um de nós deixe um "rasto digital"[8] em sistemas informáticos. Adicionalmente, tem-se assistido a uma tendência crescente do aumento de dados não só armazenados, mas também em circulação nos referidos sistemas e redes informáticas.

Neste sentido, a tecnologia acaba por ser um espelho da vida de cada um de nós e isso pode ter consequências a vários níveis, nomeadamente no âmbito do Direito Penal e do Direito Processual Penal[9]. Desde logo, é certo que, com os avanços tecnológicos, também a prática de crimes ao nível digital registou um aumento exponencial. De facto, a criminalidade informática ganhou palco e cada vez são cometidos mais crimes com recurso a estes meios. Assim, apesar de serem notórias as vantagens associadas ao progresso tecnológico[10], não podemos negar que a disponibilização e utilização crescentes das

[4] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 31
[5] CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, ano 35, n.º 139 (julho/setembro), 2014, p. 29
[6] A denominada sociedade de informação que nasceu com as novas tecnologias.
[7] Seja a nível profissional, pessoal ou familiar, seja ao nível da educação, da saúde, da ciência e até do lazer.
[8] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 32
[9] 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
[10] Nomeadamente no que diz respeito a uma melhoria da qualidade de vida que se reflete em todos os setores da sociedade.

tecnologias de informação e comunicação, com todas as suas potencialidades, têm levado ao seu uso como instrumentos privilegiados da prática de atos de elevada danosidade[11].

Daqui resultam problemas evidentes para a investigação criminal, nomeadamente no que diz respeito à obtenção de prova, visto que, como analisaremos mais adiante, os agentes da prática de crimes servem-se de técnicas cada vez mais sofisticadas que prejudicam – e, por vezes, impossibilitam – a recolha de prova.

Face a estes entraves, vários países têm procurado dotar-se de novas técnicas e novos meios de obtenção de prova que lhes permitam estar em pé de igualdade com os agentes da prática de crimes. Desta forma, tem-se entendido que, tendo em conta que estes últimos utilizam técnicas intrusivas para levar a cabo as suas atividades criminosas, também os Estados, na veste das respetivas autoridades judiciárias e órgãos de polícia criminal, devem poder socorrer-se de meios semelhantes para garantir o sucesso das suas investigações criminais[12]. Um destes métodos inovadores diz respeito à utilização de *malware* tendo em vista a obtenção de prova em processo penal e é sobre ele que recairá toda a nossa análise.

[11] MILITÃO, Renato Lopes, "A propósito da prova digital no processo penal", *Revista da Ordem dos Advogado*s, volume I, ano 72, 2012, p. 251
[12] CORREIA, João Conde, "Prova digital: as leis que temos…", cit., p. 42

2. Utilidade e relevância prática no âmbito da investigação criminal

Primeiramente, importa esclarecer o conceito de *malware*, isto é, no que consiste, quais as suas funcionalidades, qual o modo de instalação e respetivo funcionamento. Este termo resulta da junção do adjetivo *malicious* (malicioso) e do substantivo *software* (programa informático)[13], podendo ser definido, sucintamente, como um programa informático malicioso que se aproveita de uma vulnerabilidade do sistema informático ou do próprio utilizador e que é instalado[14], *in loco* ou de forma remota, no sistema informático do visado, sem o seu conhecimento e consentimento esclarecido[15].

No fundo, falamos de programas[16] instalados por terceiros, de forma sub-reptícia, num sistema informático para comprometer as suas funcionalidades, controlar acessos, monitorizar atividades, bem como para proceder à apropriação, alteração ou eliminação de dados informáticos, prejudicando o utilizador e/ou o sistema infetado[17].

Uma vez instalado, o *malware* pode levar a cabo um conjunto de medidas para permanecer indetetável[18], podendo, simultaneamente, empreender uma panóplia de tarefas tendo em conta aquilo que o atacante[19] pretende que ele faça, possibilitando a recolha de informação interna ao sistema (dados armazenados, não armazenados ou produzidos em tempo real), bem como a recolha de informação externa (através da ativação da *webcam* e/ou do microfone)[20]. A sua execução pode incluir a comunicação destes dados a uma entidade externa (OPC ou AJ) tendo em vista o seu controlo.

Posto isto, coloca-se a questão de saber por que razão a utilização de *malware* como meio de obtenção de prova pode revelar-se útil e/ou necessária ao ponto de merecer a sua previsão legal, uma vez que as entidades responsáveis pela investigação criminal têm ao seu

---

[13] RAMALHO, David Silva, "O uso de *malware* como meio de obtenção de prova em processo penal", *Revista de Concorrência e Regulação*, ano IV, n.º 16 (outubro/dezembro), 2013, p. 201

[14] Esta instalação traduz-se numa infeção do sistema por uma de três vias: suporte físico removível, *web browser* ou *download* voluntário.

[15] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., pp. 34-36

[16] O mais comum é o Cavalo de Troia, mas podemos mencionar tantos outros: *logic bombs*, *spyware*, *rootkits*, *worms*, *blended threats*, vírus.

[17] RAMALHO, David Silva, "O uso de *malware*…", cit., p. 202

[18] *Idem*, p. 207

[19] Neste caso, as autoridades judiciárias e/ou órgãos de polícia criminal.

[20] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 36

dispor, na nossa legislação processual penal atualmente em vigor, um vasto leque de opções no que diz respeito à recolha de prova.

Desde logo, e recapitulando o que já referimos anteriormente, vivemos numa sociedade dominada pelas novas tecnologias, na qual cada um de nós vai deixando a sua "pegada digital". A par disso, assistimos a uma proliferação da criminalidade informática, sendo esta marcada pela utilização de técnicas e métodos cada vez mais sofisticados e imunes a possíveis "falhas".

De facto, as novas tecnologias vieram colocar enormes dificuldades no que respeita à busca, preservação, apreensão, análise, tratamento e apresentação das provas nelas armazenadas: as chamadas provas digitais. Falamos de tecnologias que podem ser usadas à distância, sem contacto físico com os sistemas informáticos, facilitando o encobrimento dos seus utilizadores e permitindo-lhes atuar em qualquer parte do mundo sem deixar rasto.[21]

Neste contexto, nos dias de hoje, é evidente que a prova digital marca presença na maior parte dos processos penais. Mas o que é a prova digital? Embora não seja simples nem unânime a sua definição, tem um conjunto de características que a singularizam e que importa referir. Resumidamente, destaca-se pela sua imaterialidade ou invisibilidade, assim como pela sua fragilidade e volatilidade. Ademais, tal prova é composta por uma sequência de *bits* e existe independentemente do tipo de suporte físico no qual é incorporada[22]. Por fim, é uma prova que pode encontrar-se dispersa por vários locais, virtuais e geográficos[23].

Todas estas especificidades da prova digital põem em evidência a necessidade de preservação da cadeia de custódia de forma a garantir a sua autenticidade e fidedignidade[24], bem como exigem uma resposta célere e altamente qualificada que possibilite o acesso a dados que, de outro modo, seriam dificilmente acessíveis.

Assim, urge a adoção de um método científico subjacente às atividades de recolha, exame, análise e apresentação da prova digital que proporcione condições para descobrir a

[21] MILITÃO, Renato Lopes, "A propósito da prova digital no processo penal", cit., pp. 260-261
[22] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital…", cit., p. 134
[23] RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Coimbra: Almedina, 2017, pp. 102-108
[24] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital…", cit., p. 134

prova e assegurar a sua aptidão para demonstrar juridicamente os factos: este método é atualmente designado por Ciência Forense Digital[25].

Precisamente por força da evolução da Ciência Forense Digital e também da recrudescente intromissão do Estado no conteúdo das comunicações eletrónicas têm sido desenvolvidos métodos com o objetivo de frustrar a deteção, monitorização, prova ou imputação de uma atividade em ambiente digital ao seu autor. Apesar de, por um lado, se tratarem de medidas legítimas que visam garantir a segurança dos dados informáticos e a preservação do anonimato, por outro lado, consistem, simultaneamente, em meios para dissimular indícios da prática de crimes e frustrar a recolha de prova – daí que sejam denominadas de medidas anti-forenses[26].

No domínio das medidas anti-forenses, vamos debruçar-nos sobre os anonimizadores – que visam evitar a deteção da atividade criminosa – e sobre a encriptação – que se destina a evitar o exame e a análise de dados.

Quanto aos anonimizadores[27], estamos perante programas que visam permitir a navegação e atuação na Internet anónimas, impedindo os OPC de associar uma conduta *online* ao seu autor[28], ocultando a sua origem através da utilização fraudulenta de dados de identificação ou através de servidores *proxy, mix cascades* ou *onion routing*[29].

Relativamente à encriptação[30], estamos perante uma forma de dissimulação de dados que se destaca por ter um caráter potencialmente inultrapassável. Sinteticamente, diz respeito a princípios e técnicas que transformam, de forma reversível, uma informação legível em ilegível[31], de modo a protegê-la do acesso não autorizado ou de modificações por parte de terceiros, através do recurso a códigos ou chaves. Esta ciência de escrever

[25] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 109
[26] *Idem*, pp. 150-151
[27] Inicialmente, estes surgiram para acautelar a liberdade de expressão e informação dos utilizadores; contudo, passaram a ser usados para eliminar o rasto digital dos agentes da prática de crimes. Assim, RAMALHO, David Silva, "A investigação criminal na Dark Web", *Revista de Concorrência e Regulação*, ano IV, n.º 14/15 (abril/setembro), 2013, p. 392
[28] Neste campo, destaca-se o navegador *Tor*, que consiste num programa de *onion routing* que garante a confidencialidade e inviolabilidade das comunicações dos seus utilizadores, assim como o anonimato do seu remetente. O *Tor* tem um papel muito relevante no acesso à *Dark Web*. Assim, CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 46
[29] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 152
[30] Uma componente da criptografia.
[31] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 165

informação de forma secreta é, no fundo, uma concretização prática do princípio da segurança desde a conceção[32].

Nos últimos anos, tem-se assistido a um aumento da utilização desta tecnologia pelos agentes da prática de crimes. Isto é, na troca de dados, estes socorrem-se de aplicações e serviços que recorrem à chamada encriptação ponta-a-ponta na realização de comunicações, impedindo os servidores de aceder ao conteúdo das mesmas. Desta forma, as interceções de conteúdo das comunicações revelam-se, nestes casos, inúteis, o que significa que se estiverem em causa ficheiros ou comunicações com grande relevo probatório, esta técnica pode frustrar por completo o sucesso de uma investigação criminal.

Neste âmbito, cabe também destacar o recurso à *dark web* pelos agentes da prática de crimes. Esta consiste numa parcela profunda da Internet que se dedica à cibercriminalidade, onde a navegação é livre, anónima, cifrada e potencialmente indetetável e na qual todas as trocas de dados são encriptadas, não havendo acesso ao seu conteúdo, origem ou destinatários[33].

Por fim, importa ainda fazer referência aos programas autodestrutivos: estes são previamente instalados nos sistemas informáticos e ativam mecanismos de agressão às perícias forenses[34].

Todos estes obstáculos que são colocados por estas medidas anti-forenses põem em evidência a importância da utilização do *malware* como meio de obtenção de prova. De facto, o *malware* permite, desde logo, efetuar a vigilância na fonte, possibilitando o acesso aos dados antes da encriptação ou depois da desencriptação[35]. Além disso, surge como a única ferramenta capaz de ultrapassar as barreiras encriptadoras, permitindo chegar à identificação e localização do utilizador[36].

Neste sentido, parece agora evidente a utilidade e pertinência deste novo meio de obtenção de prova para a investigação criminal, uma vez que é o único a mostrar-se capaz

[32] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 43, nota 65
[33] *Idem*, p. 46
[34] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 174
[35] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 45
[36] *Idem*, p. 47

de solucionar os problemas referidos, principalmente tendo em conta o constante progresso tecnológico.

Ademais, daqui se depreende que as ações de investigação criminal relativas à prova digital exigem aprofundados conhecimentos informáticos, bem como meios técnicos e tecnológicos de ponta. Assim, reclama-se a adoção de medidas específicas e eficientes, devendo a nossa lei processual penal permitir que as entidades policiais e judiciárias possam desenvolver as ações necessárias e adequadas à obtenção de prova digital eficazmente, assim como dotar tais entidades de recursos humanos e meios técnicos capazes de dar resposta às dificuldades e complexidades com que se deparam em investigações deste tipo.[37]

[37] MILITÃO, Renato Lopes, "A propósito da prova digital no processo penal", cit., pp. 261-262

3. Integração nos métodos ocultos de investigação

Perante uma criminalidade cada vez mais complexa e excecional, é fundamental que o Estado reforce a sua atuação no que concerne à prevenção e investigação criminais, nomeadamente através do recurso a métodos ocultos de investigação[38].

De facto, ao longo da vigência do CPP, o mundo mudou, a criminalidade mudou e é evidente a disseminação das novas tecnologias e a sua aptidão para fomentar a prática de crimes, reduzindo a possibilidade de deteção dos mesmos[39]. Neste sentido alertou Anabela Miranda Rodrigues[40], afirmando que "o mundo mudou e, como nestas coisas da perseguição penal, o processo muda com o mundo, o processo penal mudou".

Assim, perante esta mudança para uma criminalidade mais complexa, marcada pela especial gravidade dos ilícitos e pela sofisticação do modo da sua execução[41], os Estados começaram a sentir necessidade de se munirem de instrumentos mais eficazes e de procederem a uma certa ocultação da investigação criminal, acabando por implementar medidas cada vez mais restritivas dos direitos dos cidadãos em virtude da consagração e do recurso a novos métodos, também eles mais gravosos e sofisticados[42].

Segundo a lição de Costa Andrade, "os métodos ocultos de investigação representam uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dele se apercebam"[43]. Assim, podemos, desde logo, verificar que o *malware* pode ser reconduzido a esta categoria doutrinal, visto que a sua introdução no sistema informático implica necessariamente a ausência de conhecimento do visado, o que evidencia a natureza oculta deste meio[44].

---

[38] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., pp. 49-50
[39] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 202
[40] RODRIGUES, Anabela Miranda, "A defesa do arguido: uma garantia constitucional em perigo no «admirável mundo novo»", *Revista Portuguesa de Ciência Criminal*, ano 12, n.º 4 (outubro/dezembro), 2002, p. 550
[41] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 204
[42] *Idem*
[43] 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: Coimbra Editora, 2009, pp. 104-105
[44] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 50

Estes meios (ocultos) de obtenção da prova reúnem um conjunto de características distintivas que revelam a sua "drástica e comprometedora danosidade social"[45]. Desde logo, são utilizados com desconhecimento do visado, o que implica que lhes seja inerente um secretismo na atuação dos poderes públicos. Além disso, são bastante abrangentes, uma vez que afetam um número elevado de pessoas e permitem recolher uma imensa quantidade e variedade de informação[46]. Por sua vez, levam à restrição de direitos fundamentais, nomeadamente de direitos processuais do arguido (*maxime* o direito à não autoincriminação). Por fim, são pautados pela sua deslealdade, na medida em que retiram ao visado a liberdade de definir os limites da sua ação.[47]

Estes métodos, ao atribuírem uma maior importância ao inquérito[48], acabam por se refletir num "desarmar" da função do juiz em prol do MP e dos OPC[49], pois como refere Costa Andrade[50], há uma "deslocação do centro de gravidade das decisões da fase do julgamento para os resultados obtidos em sede de inquérito". Ademais, conferem ao Estado uma extensa amplitude de atuação, podendo pôr em causa o estatuto processual do arguido e, assim, corroer os fundamentos do Estado de Direito Democrático[51].

Neste seguimento, podemos desde já concluir que é fundamental que o processo penal evolua e que sejam previstos e utilizados novos métodos que permitam ultrapassar as barreiras impostas por tal mudança. No entanto, é importante frisar que este recurso a novos meios não pode ser feito sem critérios, nomeadamente quando isso implique uma ingerência nos direitos fundamentais.

Assim, e acompanhando a lição de David Silva Ramalho[52], apesar de a ampliação dos meios à disposição da investigação criminal ser uma inevitabilidade, exige-se que estejam reunidos certos pressupostos para que estes possam ser utilizados, nomeadamente ao nível da necessidade do meio e da gravidade do crime. No fundo, terá de se comprovar

[45] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*"…, cit., p. 106
[46] Muitas vezes sem ter em conta a intimidade e fiabilidade da comunicação. Assim, RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 209
[47] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 51
[48] Visto ser nesta fase do processo que se obtêm os resultados das investigações ocultas.
[49] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*"…, cit., p. 107
[50] *Idem*
[51] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 51
[52] RAMALHO, David Silva, *Métodos Ocultos*…, cit., pp. 204-205

que aquele meio é necessário para a eficácia da perseguição criminal em concreto e que a gravidade do crime e o seu grau de lesividade justificam o recurso a um meio tão gravoso.

Neste sentido, importa realçar o caráter excecional e não automático[53] dos métodos ocultos de investigação criminal, cuja consagração não implica a sua utilização sem apertadas regras e limitações. Na verdade, só o facto de se tratar de métodos ocultos tem implícito um traço de danosidade, daí que seja essencial estabelecer critérios rigorosos para a sua aplicação e que fazem desta uma situação excecional. Caso contrário, não sendo cumpridos todos os requisitos exigidos, estaremos indubitavelmente perante uma situação de impossibilidade de utilização em virtude das proibições de prova.

Esta é uma temática marcada por uma "relação de permanente tensão" entre a "defesa dos cidadãos contra abusos do Estado" e a "legitimação estatal para a utilização dos meios à disposição na investigação criminal"[54], pelo que se impõe o respeito por um conjunto de princípios fundamentais para garantir a legitimação e respetiva utilização de métodos ocultos no âmbito de uma investigação criminal.

Primeiramente, convocamos o princípio da reserva de lei. Tal como dispõe o artigo 125.º do CPP[55], os meios de prova admitidos em processo penal não estão limitados pelo catálogo legal, podendo recorrer-se a meios atípicos[56] desde que estes não sejam proibidos por lei. Todavia, sabemos que, entre nós, vigora o princípio da legalidade, o que significa que a utilização desses meios atípicos deve circunscrever-se a casos excecionais e apenas na medida em que tal seja necessário por força da inaptidão de outros meios para a prova dos factos em questão[57]. Ademais, um meio de prova atípico terá sempre de passar o crivo do artigo 126.º do CPP a fim de verificar a inexistência de proibições legais expressas por restringir direitos do visado. Tudo isto permite concluir que não basta a "aparente não ilegalidade" do referido meio atípico, mas é também necessário que este seja conforme com princípios constitucionais e processuais penais em matéria probatória e de direitos fundamentais[58]. Ora, face ao exposto, e tendo em conta que a maioria dos métodos ocultos

[53] *Idem*, p. 210
[54] *Idem*, pp. 210-211
[55] Sob a epígrafe "legalidade da prova", dispõe que "são admissíveis as provas que não forem proibidas por lei.".
[56] Isto é, não previstos na lei.
[57] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 214
[58] *Idem*, p. 216

tende a restringir direitos fundamentais, é condição fundamental da legitimidade da medida e da validade da prova obtida a precedência de lei ou decreto-lei autorizado pela Assembleia da República (cf. artigos 18.º, n.º 2 e 3, e 165.º, alínea b) da CRP)[59], prendendo-se esta reserva de lei com questões de segurança jurídica[60].

Em segundo lugar, invocamos o princípio da proporcionalidade. Como defende Costa Andrade[61], na dialética entre os interesses da investigação e a restrição de direitos fundamentais, "o cumprimento da proporcionalidade obriga a chamar à balança da ponderação um largo espetro de valores e interesses", nomeadamente no que respeita ao "universo dos direitos e dos sujeitos atingidos, a eminência e dignidade dos bens jurídicos a salvaguardar e a idoneidade da medida para o conseguir". Desta forma, o sacrifício de direitos fundamentais só poderá ter lugar perante o cumprimento de critérios de proporcionalidade[62], a respeitar pelo legislador e pelo aplicador da lei[63]. Ao legislador caberá fazer uma filtragem dos crimes e das condições da sua prática suscetíveis de justificar uma concreta restrição de direitos; ao aplicador caberá aferir, baseando-se na lei e na Constituição, se em face "dos indícios, da concreta gravidade do ilícito, da necessidade da prova e da insuficiência de métodos menos gravosos para satisfazer o mesmo objetivo é ou não proporcional recorrer ao método oculto em causa", tendo em conta o grau de lesão e da danosidade social do mesmo[64].

Em terceiro surge o princípio da subsidiariedade, que consiste na ideia de que a autoridade judiciária competente dê prioridade aos métodos abertos de investigação e, só nos casos em que estes não sejam aptos para satisfazer os interesses da investigação, recorra ao método menos gravoso de entre os idóneos. No fundo, a utilização destes métodos deve ser reservada para casos graves e de extrema necessidade.[65]

Por fim, temos o princípio da reserva de juiz. De facto, sabemos que, tratando-se de uma medida que se prenda com direitos fundamentais – como é o caso dos métodos ocultos

[59] *Idem*, p. 220
[60] Nomeadamente para prevenir o arbítrio das autoridades públicas, para garantir que a comunidade conhece os meios processuais ao seu dispor e para permitir um controlo jurisdicional efetivo.
[61] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*"…, cit., p. 116
[62] Falamos do princípio da proporcionalidade em sentido amplo, que se subdivide nos princípios da adequação/idoneidade, da necessidade/exigibilidade e da proporcionalidade *strictu sensu*. Para mais desenvolvimentos: RAMALHO, David Silva, *Métodos Ocultos*…, cit., pp. 230-235
[63] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 227
[64] *Idem*, p. 229
[65] *Idem*, p. 236

de investigação –, caberá ao juiz[66], enquanto entidade independente e imparcial no processo, aferir do cumprimento dos pressupostos legais para a sua utilização e decidir pela justificação casuística da restrição de direitos fundamentais (cf. artigos 32.º, n.º 4, e 202.º, n.º 2 da CRP). No âmbito da ocultação dos métodos de investigação este papel do juiz tem uma importância acrescida, na medida em que não é assegurado o contraditório ao titular do direito restringido. [67]

[66] *Maxime* o juiz de instrução, uma vez que estas medidas têm como palco a fase de inquérito.
[67] RAMALHO, David Silva, *Métodos Ocultos…,* cit., pp. 236-237

4. O conflito entre as finalidades do processo penal

Habitualmente, apontamos três finalidades ao processo penal: a realização da justiça e descoberta da verdade material; a proteção perante o Estado dos direitos fundamentais das pessoas[68]; e o restabelecimento da paz jurídica comunitária posta em causa com a prática do crime[69].

Estas finalidades entram permanentemente em conflito, não sendo totalmente harmonizáveis, nomeadamente no que diz respeito à matéria da prova. De facto, acompanhamos a lição de Figueiredo Dias quando conclui pelo seu "caráter irremediavelmente antinómico e antitético"[70]. De acordo com o autor, esta impossibilidade de harmonização integral só pode ser superada se se "operar a concordância prática das finalidades em conflito, de modo a salvar de cada uma, em cada situação, o máximo conteúdo possível, otimizando os ganhos e minimizando as perdas axiológicas e funcionais, sempre com o limite da intocável dignidade da pessoa humana"[71].

Esta tensão dialética característica do processo penal sente-se de forma mais acentuada no domínio da prova. A título de exemplo, podemos apontar um conjunto de vantagens à introdução de um novo meio de obtenção de prova tendo em vista a descoberta da verdade material[72], como é o caso do *malware*, cuja utilização se justifica, como vimos anteriormente, para fazer face aos obstáculos colocados pelo desenvolvimento da tecnologia e pelo recurso a meios mais sofisticados pelos agentes da prática de crimes[73]. Isto é fundamental para a utilidade e eficácia da ação penal, uma vez que permite a obtenção de elementos probatórios essenciais para a investigação, respondendo às exigências comunitárias de perseguição e condenação de criminosos[74].

---

[68] Do arguido e de terceiros.
[69] ANTUNES, Maria João, *Direito Processual Penal*…, cit., p. 18
[70] 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
[71] ANTUNES, Maria João, *Direito Processual Penal*…, cit., p. 19 e DIAS, Jorge de Figueiredo, *Direito Processual Penal: Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por*…, cit., p. 25
[72] Esta pode ser entendida como um dever ético e jurídico que é objeto de interesse público e componente essencial do princípio do Estado de Direito.
[73] CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 54
[74] *Idem*, pp. 54-55

No entanto, a utilização de *malware*, assim como de qualquer outro meio oculto, implica a restrição de um vastíssimo leque de direitos fundamentais, não só do arguido, mas de um elevado número de pessoas; restrição esta especialmente intensa quando estamos no domínio do ambiente digital ou eletrónico. De facto, ao analisarmos este meio de obtenção de prova, facilmente percebemos que todas as suas funcionalidades revelam um potencial de devassa elevado[75], o que o leva a ser considerado por muitos autores como "o meio mais invasivo e mais restritivo" de todos[76].

Desde logo, o uso de *malware* permite o acesso a todos os dados armazenados, não armazenados ou produzidos em tempo real, podendo revelar aspetos relacionados com a personalidade, verificando-se assim uma restrição do direito à integridade e confidencialidade dos sistemas informáticos[77].

Por sua vez, dão-se a conhecer dados sem o consentimento livre e esclarecido do visado, retirando-lhe a possibilidade de decidir "quando e dentro de que limites os seus dados pessoais podem ser revelados"[78], sendo assim restringido o direito à autodeterminação informacional (artigos 26.º, n.º 1 e 35.º da CRP)[79]. Além disso, e neste seguimento, permite-se o acesso a dados que projetam uma "área nuclear inviolável e intangível da vida privada, protegida contra qualquer intromissão", estando em causa uma violação do direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1 e 2 da CRP)[80].

Adicionalmente, não podemos menosprezar a violação de outros direitos em certos casos, nomeadamente quando estamos perante a recolha de prova externa através da ativação de *hardware*: o direito à palavra e o direito à imagem quando se recorre ao microfone e à câmara (artigo 26.º, n.º 1 da CRP), assim como, em situações mais específicas, o direito à inviolabilidade do domicílio (artigo 34.º, n.º 2 da CRP) [81].

---

[75] *Idem*, pp. 55-56
[76] RAMALHO, David Silva, *Métodos Ocultos*…, cit., pp. 354
[77] Este foi desenvolvido pela jurisprudência alemã e visa proteger contra o acesso oculto a qualquer sistema de tecnologia de informação, podendo ser abrangido pela proteção do artigo 26.º, n.º 1 da CRP (direito ao desenvolvimento da personalidade). Assim, CAMPOS, Juliana, *O malware como meio de obtenção da prova…*, cit., p. 57
[78] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital…", cit., p. 138
[79] *Idem*, p. 58
[80] *Idem*, pp. 58-59
[81] Para mais desenvolvimentos sobre este ponto: CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 60 e ss.

De facto, face ao exposto, parece-nos evidente que o direito ao livre desenvolvimento da personalidade, projetado em todos estes direitos elencados e protegido constitucionalmente, se encontra bastante comprometido. Mais, é evidente o desequilíbrio entre as finalidades do processo penal, uma vez que assistimos a uma propensão no sentido de garantir a descoberta da verdade material e a realização da justiça em prejuízo da proteção dos direitos fundamentais das pessoas.

Neste sentido, cabe ao legislador encontrar o dito "ponto de concordância prática"[82] de forma a harmonizar as referidas finalidades. Isto é, o *malware* surge, efetivamente, como um meio útil e eficaz para a perseguição penal, visto ser imprescindível para ultrapassar certas barreiras que, de outro modo, seriam intransponíveis. No entanto, estamos perante um meio que, pelas suas características e nível de lesividade, não pode ser admitido a todo o custo, mesmo que em nome da descoberta da verdade. Assim, é fundamental encontrar um ponto de equilíbrio que permita, por um lado, potenciar a utilização deste meio no sentido de ter acesso a elementos probatórios essenciais e inacessíveis de outra forma e, por outro lado, garantir, simultaneamente, a proteção adequada dos direitos fundamentais que podem ser postos em causa com a sua utilização.

Este ponto de equilíbrio entre os interesses da investigação e a proteção dos direitos fundamentais terá de se refletir em normas processuais que definam certos limites que são, em algumas situações, inultrapassáveis – como é o caso da dignidade da pessoa humana –, mas que também são superáveis em outras ocasiões, desde que cumpridos certos requisitos[83].

Em suma, e acompanhando a lição de David Silva Ramalho, podemos afirmar que a instalação de *malware* será, possivelmente, "o meio mais gravoso de obtenção de prova suscetível de merecer consagração legal num Estado de Direito democrático". Este método destaca-se claramente pelo seu nível de danosidade social, ofendendo gravemente os direitos fundamentais à reserva da intimidade da vida privada, à inviolabilidade do domicílio, à privacidade, à imagem, à palavra e à confidencialidade e integridade dos sistemas

[82] DIAS, Jorge de Figueiredo, *Direito Processual Penal: Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por*…, cit., p. 25
[83] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 67-68

informáticos[84]. Desta forma, a sua consagração legal tem de ser densificada, estabelecendo limites claros e específicos que respeitem o princípio da proporcionalidade[85].

[84] RAMALHO, David Silva, "O uso de *malware*…", cit., p. 233
[85] *Idem*

CAPÍTULO II

A PREVISÃO E O USO DE *MALWARE* NOUTROS ORDENAMENTOS JURÍDICOS E EM PORTUGAL

1. A previsão e o uso de *malware* nos ordenamentos jurídicos estrangeiros

Desde os finais dos anos noventa que temos assistido à utilização do *malware*, por parte dos OPC e das AJ de vários países, como método oculto de investigação, de modo a ultrapassar as dificuldades que temos vindo a enunciar[86]. Neste sentido, o elevado potencial deste método tem conduzido a que vários ordenamentos jurídicos o tenham consagrado legal ou jurisprudencialmente[87], o que se tem traduzido naquilo a que podemos chamar de "movimento de positivação do *malware*" em alguns países, principalmente na última década, ainda que com designações distintas[88]. Assim, parece-nos pertinente fazer uma breve referência a alguns destes ordenamentos jurídicos.

No ordenamento jurídico espanhol, os *registros remotos sobre equipos informaticos* encontram-se previstos nos arts. 588 *spties* a, b e c da LECrim[89], tendo sido legitimados através de duas medidas distintas: o *hacking* (através da utilização de dados e códigos de identificação) e o *malware* (através da instalação de *software*) [90], que, quando utilizados remotamente e sem conhecimento do proprietário ou utilizador, terão de ser autorizados pelo juiz e apenas quando esteja em causa a investigação dos crimes referidos na respetiva norma[91].

---

[86] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 105
[87] RAMALHO, David Silva, *Métodos Ocultos*…, cit., pp. 324-325
[88] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 105
[89] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, 2.ª Edição Revista e Atualizada, Coimbra: Gestlegal, 2021, p. 484
[90] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 107-108
[91] Tais como: crimes cometidos no âmbito de organizações criminosas, de terrorismo, de crimes cometidos contra menores ou incapazes, contra a Constituição, de traição e relativos à defesa nacional ou de crimes cometidos com utilização de meios informáticos ou de qualquer outra tecnologia da informação ou das comunicações ou serviço de comunicações. Assim, NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., p. 485

No ordenamento jurídico italiano, o recurso ao *malware* está consagrado no art. 266, 2 e 2-bis do *Codice di procedura penale*, que prevê o uso do *captatore informatico*, isto é, um *software* do tipo Cavalo de Troia que é instalado, de modo sub-reptício, num sistema informático para permitir a ativação do microfone para audição/gravação de conversações, geolocalização e ativação da câmara[92]. Neste caso, constitui um meio de execução da interceção de comunicações entre presentes e não um meio autónomo, tendo esta de ser autorizada pelo juiz[93].

No ordenamento jurídico alemão, este método sempre se considerou previsto, não como meio de prossecução penal, mas de defesa contra os perigos e de prevenção contra crimes[94]. Todavia, a ausência de regulação específica não impedia as autoridades de o utilizarem no âmbito do processo, o que levava a divergências jurisprudenciais[95]. Assim, foram introduzidas duas medidas: a *Online Durchsuchung* ("busca *online*" com duas modalidades: 1) um único acesso e 2) monitorização a longo prazo); e a Quellen-TKU ("vigilância na fonte")[96].

Por fim, dedicar-nos-emos a uma análise mais profunda ao ordenamento jurídico americano por razões que se prendem, desde logo, com a vasta e já longa utilização deste método por parte das autoridades no âmbito das suas investigações. Além disso, uma vez que, mais à frente, abordaremos uma operação de sucesso impulsionada pelos EUA, importa clarificar a experiência americana no que toca à utilização de *malware*. De facto, até ao momento, não existe, no direito norte-americano, legislação específica relativa à utilização

[92] *Idem*, p. 490
[93] *Idem*, pp. 490-491
[94] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 110
[95] Antes da entrada em vigor da atual legislação, o *malware* estava previsto apenas no âmbito da prevenção criminal; ao nível da repressão criminal, a lei não o regulava e não existia unanimidade na jurisprudência alemã, sendo que uns se pronunciavam pela sua admissibilidade, aplicando o regime das buscas com base numa interpretação atualista e outros pronunciavam-se pela sua inadmissibilidade por ausência de previsão legal. No entanto, "a Sentença do Bundesverfassungsgericht (Tribunal Constitucional Federal alemão) de 27/02/2008 considerou que, no uso de *malware*, os direitos fundamentais ao sigilo das telecomunicações, à inviolabilidade do domicílio e à autodeterminação informacional não proporcionavam uma tutela eficaz e, por isso, criou um novo direito fundamental (que entendeu ser restringido, de forma intensa, pelo *malware*): o direito fundamental à confidencialidade e integridade dos sistemas técnico-informacionais. Mais, considerou que só seria legítimo o recurso ao *malware* mediante autorização judicial e desde que exista suspeita fundada da existência de um perigo concreto para um bem jurídico particularmente relevante, devendo a lei conter salvaguardas para proteção da área nuclear da privacidade.". Assim, NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., pp. 482-483, nota 1099
[96] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 111-112

deste meio de obtenção de prova no âmbito de uma investigação criminal[97]. Não obstante, o recurso a este meio tem feito parte da *praxis* jurídica[98], havendo registo da sua utilização por parte das entidades policiais[99].

O primeiro caso conhecido de utilização de *malware* pelas forças policiais nos EUA é o Caso *Scarfo*[100], que remonta a 2000, quando agentes do FBI realizaram uma busca ao escritório de Nicodemo S. Scarfo e de Frank Paolercio, com o objetivo de recolherem provas de uma operação de jogo ilegal e agiotagem. No decurso desta, encontraram um computador pessoal que pertencia aos suspeitos, no qual estava armazenado um ficheiro intitulado de "Factors", indecifrável sem a palavra-passe. Neste sentido, em maio do mesmo ano, o FBI muniu-se de dois mandados – um para aceder novamente ao local e outro para aceder ao sistema informático – e regressou ao escritório, instalando no referido computador um sistema de *hardware/software* e/ou *firmware*, designado de *Key Logger System* (KLS) que tinha como função registar as teclas premidas no computador. Pouco depois, o FBI conseguiu obter a palavra-passe e decifrar o ficheiro encriptado, no qual encontrou registos das operações ilegais que permitiram uma posterior acusação dos suspeitos pela prática dos crimes de jogo ilegal e agiotagem.

Um outro exemplo foi o *Magic Lantern*, que correspondia a um *keylogger* concebido para ser instalado[101], de forma remota e sub-reptícia, no sistema informático do visado, em caso de suspeita de envolvimento em atividades criminosas. Anos mais tarde, este veio a ser substituído pelo CIPAV (*Computer and Internet Protocol Address Verifier*): um tipo de *malware* que reunia um conjunto bastante alargado de funcionalidades, permitindo aceder ao endereço IP e/ou MAC, bem como à localização, aos programas em funcionamento, ao sistema operativo, à conta de utilizador aberta ou ao último *website* visitado. Este foi um

[97] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., p. 486
[98] Neste sentido se pronunciou a Procuradora Geral Adjunta da Divisão Criminal do Departamento de Justiça, Leslie R. Caldwell, afirmando que "O uso de buscas remotas não é novo e os mandados de buscas remotas são atualmente emitidos de acordo com a Regra 41", disponível em <https://www.justice.gov/archives/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation> (consultado a 15/06/2022)
[99] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 113
[100] QUINLAN, Sayako/WILSON, Andi, "*A Brief History of Law Enforcement Hacking in the United States*", 2016, p. 3, disponível em <https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf> (consultado a 15/06/2022)
[101] Este podia ser instalado através da abertura de anexos em mensagens de correio eletrónico ou através da exploração de vulnerabilidades nos sistemas operativos. RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 325

programa bastante utilizado pelas forças policiais norte-americanas, gerando uma grande discussão sobre a existência de requisitos legais[102] para a sua admissibilidade.

Mais recentemente (2012), destaca-se a famosa Operação Torpedo[103]. O caso ficou conhecido em 2013, quando se tornou pública uma ordem judicial na qual foi negada autorização judicial para a utilização de um tipo de *malware* no decurso de uma investigação criminal. Estavam em causa duas condutas: 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* idêntica àquela para se proceder a uma ordem de transferência da conta bancária do indivíduo para um banco estrangeiro.

Este novo tipo de *malware* abrangia um variado leque de funcionalidades, permitindo recolher registos da atividade na Internet[104], controlar remotamente o sistema visado, gerar coordenadas de latitude e longitude ou aceder à *webcam*.

Este pedido foi feito ao abrigo do regime aplicável às buscas e apreensões da *Rule 41* das *Federal Rules of Criminal Procedure* (FRCP), sustentando a ideia de que a instalação de *malware* era enquadrável no conceito de busca e a extração e envio de informações remotamente era enquadrável no conceito de apreensão. Já antes se admitia o recurso a este método desde que tal não violasse a Quarta Emenda à Constituição[105].

Neste caso concreto, o Tribunal afastou, desde logo, a sua competência territorial, por entender que os dados estavam armazenados em sistemas informáticos concretos, sujeitos às regras dos Estados em que se encontravam.

Relativamente aos requisitos da Quarta Emenda, a Jurisprudência do *Supreme Court* entendia que só existiria violação quando a busca e/ou apreensão implicassem a entrada

---

[102] Alguns entendem que não é necessário qualquer procedimento legal para a sua utilização, enquanto outros defendem que a mesma depende de autorização judicial. RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 326

[103] THOMPSON II, Richard M., "Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure", *Congressional Research Service*, 8 de setembro de 2016, pp. 2-3, disponível em <https://fas.org/sgp/crs/misc/R44547.pdf> (consultado a 15/06/2022) e ainda <https://www.wired.co.uk/article/operation-torpedo-fbi> (consultado a 15/06/2022). Além disso, sobre este ponto, ver decisão disponível em <https://pt.scribd.com/doc/137842124/Texas-Order-Denying-Warrant> (consultado a 15/06/2022)

[104] *Firewall*, *browser*, *cookies*, páginas favoritas, termos de pesquisa, nomes de utilizador e palavras-passe gravadas, contactos e conteúdo de correio eletrónico, *chats*, fotografias. RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 327

[105] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., p. 486

física em propriedade alheia[106]. Contudo, o mesmo Tribunal abandonou essa posição e ampliou o âmbito de proteção da Quarta Emenda, entendendo que a referida tutela incluía também a interceção e gravação de conversações e comunicações, abrangendo também pessoas, desde que estas tivessem, em concreto, uma expectativa razoável de privacidade[107]. Assim, quanto à utilização de *malware* em específico, tem-se entendido que se integra no âmbito de proteção da Quarta Emenda no que respeita à privacidade pessoal, pelo que os "cidadãos dos EUA têm uma expectativa razoável de privacidade relativamente aos seus sistemas e dados informáticos"[108].

Neste ponto, o Tribunal entendeu que o *malware* não oferecia garantias de que seria recolhido apenas o mínimo necessário de dados, nem permitia garantir que apenas os visados seriam alvo da medida[109]. Além disso, concluiu que a ativação da câmara é materialmente uma atividade de videovigilância, obrigando à verificação de pressupostos adicionais de indispensabilidade e imposição de limites à sua utilização[110].

Por fim, no que respeita à *Rule 41* das FRCP, cabe dizer que este preceito foi alterado em dezembro de 2016, passando a fazer menção expressa a buscas para acesso remoto em certas situações, daí que algumas vozes se tenham pronunciado no sentido da admissibilidade do recurso ao *malware* com base nesta norma[111]. No entanto, acompanhamos Juliana Campos no entendimento de que esta é uma posição criticável, na medida em que o referido preceito está previsto para buscas e apreensões tradicionais e menos invasivas, em locais físicos, sendo controverso legitimar a utilização de um meio tão restritivo e abrangente com base numa certa analogia com buscas remotas[112].

---

[106] Olmstead v. United States (1928) e Goldman v. United States (1942) do *Supreme Court of the United States*, disponíveis em <https://supreme.justia.com/cases/federal/us/277/438/> e <https://supreme.justia.com/cases/federal/us/316/129/> (consultado a 16/06/2022)

[107] Katz v. United States do *Supreme Court of the United States* (1967), disponível em <https://supreme.justia.com/cases/federal/us/389/347/> (consultado a 16/06/2022)

[108] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., p. 487 e Autor desconhecido, "Protecting Pivacy Under the Fourth Amendment", *The Yale Law Journal*, n.º 2, vol. 91, 1981, p. 313-314, disponível em <https://openyls.law.yale.edu/handle/20.500.13051/16120> (consultado a 16/06/2022)

[109] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 328

[110] *Idem*

[111] Cf. nota 98

[112] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 114, nota 387

Todavia, admitindo-se a utilização de *malware* ao abrigo do regime previsto na *Rule 41*, importa esclarecer que conclusões podemos retirar da aplicação dos requisitos deste regime jurídico.

Em primeiro lugar, este preceito não apresenta um catálogo de crimes, o que significa que, para se poder obter um mandado de busca, tem de se atender à Quarta Emenda da Constituição[113], que estabelece que se devem cumprir dois requisitos para que este seja admissível: a *probable cause* (causa provável)[114] e a *particularity* (particularidade).

Quanto à verificação em concreto da suspeita do crime e determinação do alvo, é de realçar que, estando o mandado de busca dependente da existência de causa provável, o requerente tem de apresentar factos suficientes para que o juiz a possa determinar e, por sua vez, aplicar a *Rule 41*. Além disso, atendendo à particularidade, o requerente tem ainda de identificar o sistema informático alvo do mandado.

Relativamente à delimitação do âmbito funcional, de acordo com a redação da norma[115], a utilização de *malware* apenas se deve destinar à recolha de prova interna ao sistema (isto é, aos dados armazenados).

Passando para o âmbito espacial, destaca-se que não é feita qualquer referência ou exigência especial quanto à utilização de *malware* no domicílio. Contudo, para que o mandado de busca remota preenchesse o requisito da particularidade, exigido pela Quarta Emenda, teria de referir o local da mesma. Claro é que esta exigência gerou problemas ao nível da determinação espacial, uma vez que, com as novas tecnologias e os avanços da criptografia, o local da busca é, na maioria das vezes, muito difícil ou impossível de determinar, pelo que este foi um dos motivos das alterações recentes ao preceito[116].

---

[113] Esta estabelece "o direito do povo de estar seguro nas suas pessoas, casas, papéis e bens, contra buscas e apreensões injustificadas" e dispõe que "nenhum mandado será emitido, a não ser por causa provável, apoiada por juramento ou afirmação, e particularmente descrevendo o local a ser revistado e as pessoas ou coisas a serem apreendidas." (<https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv>, consultado a 16/06/2022)

[114] Esta pode ser definida como as circunstâncias objetivas suficientes para criar a convicção de que irão ser encontradas informações relevantes para a investigação no sistema informático. Assim, NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., p. 489

[115] Esta refere-se a um "mandado para usar o acesso remoto para pesquisar meios de armazenamento eletrónico e apreender ou copiar eletronicamente informações armazenadas". THOMPSON II, Richard M., "Digital Searches and Seizures…", cit., p. 9, disponível em <https://fas.org/sgp/crs/misc/R44547.pdf> (consultado a 15/06/2022)

[116] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 129-130

No âmbito temporal, o mandado tem a duração máxima de catorze dias quando a apreensão do dispositivo ou cópia da informação sejam realizadas no local em que se encontram; se a cópia for posterior, fora do local (que é o mais comum no que diz respeito à utilização de *malware*), em princípio, não se exige esse prazo[117]. No primeiro caso, findo esse período, deve haver lugar a nova autorização ou desinstalação[118].

Além de todos estes aspetos, parece importante referir que, na norma em questão, não é feita qualquer referência a medidas para garantir o contraditório ou relativas ao respeito pelos princípios da proporcionalidade e subsidiariedade, bem como à salvaguarda da área nuclear da intimidade[119].

Por fim, no que concerne a requisitos orgânicos, a *Rule 41* exige que, para que seja admissível a utilização de *malware*, seja emitido, como referimos acima, um mandado de busca pelo juiz, solicitado por um agente federal do governo ou um procurador[120].

[117] *Idem*, p. 132
[118] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., p. 490
[119] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 136 e 141
[120] *Idem*, p. 144

2. A previsão do *malware* no ordenamento jurídico português

A previsão do *malware* no nosso ordenamento jurídico – ou a ausência desta – tem sido motivo de debate e discórdia entre alguns autores. Por um lado, temos um conjunto de teses que sustentam que este meio de obtenção de prova já está regulado no nosso ordenamento jurídico, encontrando previsão em normas que disciplinam o uso de outros meios. Por outro lado, temos posições que sustentam o contrário – tal como a nossa –, por entenderem que um método tão intrusivo e restritivo dos direitos fundamentais como este nunca poderá ter como fundamento legal uma remissão, fusão ou analogia relativamente a outros preceitos.

Antes de mais, importa esclarecer que o recurso a *malware*[121] como meio de obtenção de prova não está previsto na lei processual penal vigente[122]; a questão que se coloca é a de saber se está ou não previsto na Lei do Cibercrime.

A propósito disto, antes de avançarmos, é também importante referir que, a 20 de maio de 2009, deu entrada no Parlamento a Proposta de Lei n.º 289/X (4.ª) que tinha na base a pretensão da Convenção sobre Cibercrime do Conselho da Europa de harmonizar as legislações nacionais, favorecer a cooperação internacional e simplificar as investigações criminais, recorrendo a novos métodos quando necessário. A proposta baixou à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias e foi votada a 1 de julho de 2009 na Reunião de Comissão n.º 137. O relatório referente a esta foi enviado ao Presidente da República e seguiu-se a sua discussão na generalidade.

Nesta discussão[123], o Senhor Deputado Fernando Negrão (PSD) questionou o Senhor Secretário de Estado acerca da razão para o diploma não incluir a possibilidade de as entidades de investigação introduzirem no sistema informático sob investigação um "cavalo de Troia informático" de modo a obter informação contínua e em tempo real. Não tendo obtido resposta, o Senhor Deputado reiterou a questão, tendo-lhe sido respondido que o Senhor Secretário de Estado já não teria tempo para responder, podendo eventualmente

[121] Alguns autores referem-se a "buscas *online*", mas preferimos manter a designação utilizada até agora.
[122] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*"…, cit., p. 150
[123] Diário da Assembleia da República, I Série, n.º 102/X/4, de 10-07-2009, p. 40-45, disponível em <https://debates.parlamento.pt/catalogo/r3/dar/01/10/04/102/2009-07-09/40?pgs=40-45&org=PLC&plcdf=true> (consultado a 09/05/2022)

retomar a questão na discussão na especialidade. Porém, a questão colocada pelo Senhor Deputado não foi mais suscitada, não tendo sido dada nenhuma resposta acerca da hipótese de as entidades de investigação criminal recorrerem ao uso de *malware* para obtenção de prova.

Todavia, como já referimos, no que à regulação deste meio de obtenção de prova diz respeito, temos vozes que se erguem no sentido da existência de norma(s) habilitante(s) e vozes que se opõem a esta ideia. Daqui em diante dedicar-nos-emos à exposição dos argumentos sustentados por ambas as partes.

2.1. A existência de norma(s) habilitante(s)

A primeira hipótese diz respeito à aplicação do regime da interceção de comunicações[124], consagrado no artigo 18.º da LC. Este meio está previsto para as comunicações telefónicas e, por extensão, para outro tipo de comunicações eletrónicas[125], o que significa que também é aplicável à interceção de mensagens de correio eletrónico ou até de mensagens trocadas através de processos de comunicação instantânea[126].

Uma outra hipótese corresponde à "fusão" deste meio de obtenção de prova com outros regimes. Desde logo, há quem defenda um enquadramento no regime das apreensões, sendo que a LC distingue entre apreensão de dados informáticos (artigo 16.º) e apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17.º).

---

[124] Aqui, coloca-se a hipótese de se tratar de uma aplicação direta do regime do artigo 18.º da LC, bem como "retalhar", por via interpretativa, a aplicação deste regime com outros, tais como o registo de voz e imagem previsto na Lei n.º 5/2002, de 11 de janeiro e o regime das ações de prevenção previsto na Lei n.º 36/94, de 29 de setembro. Assim, RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 339

[125] Conforme já resultava da extensão prevista no artigo 189.º do CPP. Assim, VERDELHO, Pedro, "A nova Lei do Cibercrime", *Scientia Ivridica – Revista de Direito Comparado Português e Brasileiro*, 320 (outubro/dezembro), 2009, p. 746. Neste âmbito, tanto o artigo 18.º da LC, como o artigo 189.º do CPP admitem a interceção de comunicações eletrónicas, havendo alguns autores que entendem que o primeiro veio revogar parcialmente o segundo. Assim, MESQUITA, Paulo Dá, "Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal português – o Código e a Lei do Cibercrime", *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Coimbra Editora, 2010, pp. 102-105. No entanto, entendemos que há uma relação de complementaridade entre os dois artigos, na medida em que o art. 18.º da LC permite a interceção quanto aos crimes previstos na LC, consistindo, no fundo, num regime especial face ao art. 189.º do CPP. Assim, VERDELHO, Pedro, "A nova Lei do Cibercrime", cit., pp. 746-747. Neste sentido, a análise que faremos valerá para ambos os preceitos.

[126] VENÂNCIO, Pedro Dias, *Lei do Cibercrime: anotada e comentada*, Coimbra: Coimbra Editora, 2011, p. 119

Por outro lado, alguma doutrina sustenta que a utilização de *malware* está consagrada no artigo 15.º da LC que prevê a pesquisa de dados informáticos[127]. De facto, podemos destacar alguns pontos de aproximação entre este meio de obtenção de prova e o uso de *malware*. Desde logo, ambos visam obter dados que se encontram em sistemas informáticos e ambos podem ser realizados presencialmente (artigo 15.º, n.º 1) ou remotamente (artigo 15.º, n.º 5)[128]. Por sua vez, ambos podem surgir como métodos ocultos: no caso da pesquisa, referimo-nos ao caso específico do artigo 15.º, n.º 3, que permite aos OPC proceder à mesma sem prévia autorização da autoridade judiciária nas situações previstas na lei[129]. Por último, outro ponto em comum é o facto de ambos representarem um enorme grau de devassa da vida privada[130].

Paulo Pinto de Albuquerque considera que, com este preceito, o legislador quis introduzir no nosso ordenamento jurídico a utilização de *malware*, ao qual se refere como "busca *online*"[131]. Esta pode ser entendida como uma "infiltração clandestina num sistema informático para observação da sua utilização e leitura dos dados nele armazenados"[132], sendo efetuada *online*, com recurso a meios técnicos, procedendo-se à instalação sub-reptícia de um programa informático do tipo "Cavalo de Troia" no referido sistema[133].

O autor, apesar de entender que estão reunidos os pressupostos para esta consagração, adianta ainda que a lei, ao prever a possibilidade de uma pesquisa informática, não coloca restrições quanto ao conteúdo dos dados que podem ser alvo da mesma, nem exige que esta, sendo ordenada pelo MP ou pelos OPC, seja validade pelo juiz. Neste seguimento, acaba por concluir pela eventual inconstitucionalidade do preceito, apontando como desproporcional

[127] Esta visa obter dados informáticos específicos e determinados, armazenados num sistema informático (artigo 15.º, n.º 1), podendo a pesquisa inicial ser estendida a dados que se encontrem noutro sistema ou numa parte diferente do sistema pesquisado, acessíveis a partir do primeiro (artigo 15.º, n.º 5).
[128] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 83
[129] *Idem*, pp. 84-85
[130] *Idem*, p. 86
[131] ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4.ª Edição Atualizada, Lisboa: Universidade Católica Editora, 2011, p. 502
[132] ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado"*…, cit., p. 166, ANDRADE, Manuel da Costa, "Comentário ao artigo 194.º", in *Comentário Conimbricense do Código Penal: Parte Especial* (dir. Jorge Figueiredo Dias), T. I, 2.ª Edição, Coimbra: Coimbra Editora, 2012, p. 1103 e ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República…*, cit., pp. 502 e 541
[133] *Idem*

a invasão da privacidade do visado, por força dos artigos 26.º, n.º 1 e 2 e 32.º, n.º 4 da CRP, que reservam ao juiz os atos instrutórios que contendam com estes direitos afetados[134].

Duarte Rodrigues Nunes é também defensor da tese que sustenta que o artigo 15.º da Lei do Cibercrime é a norma que permite o recurso à busca *online*[135]. Todavia, o autor distingue duas hipóteses: os casos em que a introdução no sistema informático consiste num único acesso e as situações em que essa infiltração ocorre de forma contínua e prolongada no tempo[136].

Relativamente aos casos em que estamos perante um único acesso ao sistema informático, o autor apresenta um conjunto de argumentos que sustentam a admissibilidade deste meio de obtenção de prova à luz do artigo 15.º da LC.

Desde logo, e no que diz respeito à argumentação no sentido da falta de previsão legal deste método, o autor refuta esta ideia, realçando que a lei não faz distinção entre pesquisas presenciais e *online*, prevendo mesmo um caso forçoso de pesquisa remota no artigo 15.º, n.º 5 da LC[137]. Mais: sendo que a busca *online* não implica a entrada no local em que se encontra o sistema, nem a apreensão do mesmo, acaba por ser menos lesiva dos direitos fundamentais do que a pesquisa presencial[138]. Por sua vez, Duarte Rodrigues Nunes considera que a busca *online* é uma forma de efetivação de uma pesquisa, não exigindo a lei que as diligências investigatórias sejam levadas a cabo com conhecimento do visado, pelo que se admite o seu caráter oculto[139]. Além disso, considera que a instalação de *malware*[140] é um ato preparatório da pesquisa que é realizada remotamente, reforçando que a restrição de direitos neste âmbito é pouco significativa[141]. Neste seguimento, o autor conclui que este regime contém as "suficientes salvaguardas" no que toca à restrição de direitos fundamentais[142].

---

[134] ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal: à luz da Constituição da República…*, cit., p. 502
[135] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., p. 511
[136] *Idem*, p. 481
[137] *Idem*, p. 497
[138] *Idem*, p. 498
[139] *Idem*, p. 499
[140] O autor utiliza a expressão "*benware*" para designar estes programas informáticos quando são usados para fins de prevenção ou repressão criminais pelas autoridades. Assim, NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., pp. 369-370
[141] *Idem*, p. 500
[142] *Idem*, p. 501

Quanto aos casos que correspondem a um acesso continuado e prolongado no tempo, Duarte Rodrigues Nunes entende que a danosidade, em termos de restrição de direitos, é idêntica à verificada na interceção de comunicações eletrónicas, uma vez que estamos perante situações em que se procede a uma monitorização, em tempo real, de dados informáticos e da navegação *online*[143]. Neste sentido, e face ao exposto, o autor sustenta que se deve operar uma interpretação conforme à Constituição, de forma a apenas serem admissíveis as buscas *online* nesta segunda vertente nos casos em que seja igualmente admissível recorrer e, por sua vez, aplicar o regime da interceção de comunicações, previsto no artigo 18.º da Lei do Cibercrime[144].

Em suma, o autor não deixa de referir a importância de existir uma previsão expressa, por parte do legislador português, da possibilidade de lançar mão deste meio de obtenção de prova, nas duas vertentes acima referidas. No entanto, reitera a sua posição, frisando que estamos perante um "meio extremamente eficaz e necessário"[145] face à presença das novas tecnologias no nosso quotidiano, nos mais variados domínios da vida, designadamente no que toca à criminalidade, bem como aos entraves colocados à investigação criminal em virtude dos progressos tecnológicos e das medidas anti-forenses[146].

Ademais, salienta um conjunto de vantagens associadas a este método, tais como: permitir monitorizar a navegação *online*, podendo mesmo ser a única forma de o conseguir quando se trata de navegações na *dark web*; obter *passwords* e analisar o sistema em funcionamento; aceder a outros suportes informáticos; apreender ficheiros que apenas estão no sistema durante um certo período de tempo; suprir as insuficiências da intervenção nas comunicações; bem como o facto de não advertir os investigados de que estão a ser alvo de uma investigação criminal devido ao seu caráter oculto[147].

Em conclusão, Duarte Rodrigues Nunes considera que a norma que permite o recurso às buscas *online* em qualquer uma das modalidades é o artigo 15.º da LC pelos motivos expostos. Contudo, o autor destaca que, em primeira instância, deve utilizar-se este método

[143] *Idem*, p. 502
[144] *Idem*
[145] *Idem*
[146] *Idem*, pp. 503-504, ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado"*…, cit., pp. 166-167 e CORREIA, João Conde, "Prova digital: as leis que temos…", cit., p. 44
[147] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., pp. 503-506

na primeira vertente apresentada (isto é, através de um único acesso), aplicando-se, nestes casos, o regime da pesquisa de dados informáticos (artigo 15.º da LC); e, nos casos em que este não seja suficiente para obter as informações necessárias – e apenas nestes –, deverá então ser possível recorrer às buscas *online* de modo contínuo e prolongado no tempo, sendo aplicável, nestas situações, o regime da interceção de comunicações (artigo 18.º da LC)[148].

Por fim, outra parte da doutrina considera que o recurso ao *malware* está consagrado no artigo 19.º da LC que disciplina as ações encobertas. No fundo, o legislador introduziu esta norma na LC, especificamente dedicada às ações encobertas em ambiente digital[149], como forma de alargar o âmbito de aplicação da Lei das Ações Encobertas[150].

Desta forma, estamos perante ações levadas a cabo por funcionários de investigação criminal ou terceiros, sob o controlo da Polícia Judiciária, que atuam para prevenção e repressão dos crimes catalogados nas referidas leis, ocultando a sua qualidade e identidade (artigo 1.º, n.º 2 da LAE)[151]. Neste âmbito, segundo a doutrina maioritária, na categoria dos "homens de confiança"[152] serão apenas admissíveis os agentes encobertos ou infiltrados e não os agentes provocadores[153], o que significa que os primeiros terão de se dedicar apenas à recolha de informação, não provocando a prática do crime[154]. De facto, podemos observar algumas semelhanças entre o uso de *malware* e as ações encobertas em ambiente digital, nomeadamente o seu caráter oculto e o elevado potencial de devassa[155].

De acordo com David Silva Ramalho[156], o recurso ao *malware* está previsto no artigo 19.º da LC, no seu n.º 2, quando o legislador se refere a "meios e dispositivos informáticos". O autor reconhece que se trata de uma disposição vaga e pouco clara; no entanto, baseia a sua análise na ideia de que os "meios e dispositivos informáticos" mencionados pelo

[148] *Idem*, pp. 510-511
[149] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 303
[150] Lei n.º 101/2001, de 25 de agosto. Neste sentido, SOUSA, Susana Aires de, "Ações encobertas (e outras figuras próximas) na investigação da criminalidade económico-financeira", *Julgar*, n.º 38 (maio/agosto), 2019, pp. 37-38 e RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 303
[151] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 92
[152] SOUSA, Susana Aires de, "*Agent provocateur* e meios enganosos de prova. Algumas reflexões", *Separata de Liber Discipulorum para Jorge de Figueiredo Dias*, Coimbra: Coimbra Editora, 2003, p. 1221
[153] *Idem*, p. 1231
[154] *Idem*, pp. 1221-1222
[155] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 94
[156] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 343 e ss.

legislador não correspondem a meios de obtenção de prova já previstos no nosso ordenamento jurídico, servindo antes para "colmatar a insuficiência dos meios existentes"[157].

O autor reforça a sua posição acrescentando que o preceito, além de adotar uma terminologia idêntica a outros ordenamentos jurídicos que consagram o *malware*, remete para o regime da interceção de comunicações "naquilo que for aplicável", o que evidencia que os meios e dispositivos em causa não coincidem com aquela[158].

A análise de David Silva Ramalho conclui que estamos perante um "novo meio (oculto) de obtenção de prova" e um "meio particularmente gravoso de investigação"[159]. Neste sentido, terá de se tratar de um meio cujo uso se encontre limitado a situações extremamente excecionais, como é o caso das ações encobertas. Mais, importa sublinhar que os tais meios e dispositivos informáticos só serão utilizados "se necessário" e "se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter", estando dependente de despacho fundamentado do juiz de instrução (artigo 18.º, n.º 2, aplicável *ex vi* artigo 19.º, n.º 2 da LC)[160].

Em síntese, nesta linha de pensamento, os "meios e dispositivos informáticos" previstos pelo legislador no preceito em apreço dizem respeito a meios "cujo caráter excecional e invasivo possa ser comparado e condicionado ao recurso ao agente encoberto" e que devem ser "utilizados quando a própria ação encoberta e os demais métodos ocultos forem incapazes de dar resposta às exigências da investigação"[161]. Com efeito, trata-se, na visão do autor, da consagração da utilização de *malware* como método oculto de investigação criminal em ambiente digital, no contexto de ações encobertas[162].

---

[157] *Idem*, p. 344. Contudo, nem sempre o autor defendeu esta perspetiva de forma tão afincada. De facto, em 2013, quando se pronunciou sobre a possibilidade da previsão do uso de *malware* neste preceito, entendeu que o elevado grau de danosidade social e de ofensa dos direitos fundamentais propiciados por este meio exigia uma consagração legal densa e detalhada quanto às suas funcionalidades. Com efeito, considerou que este dever de precisão legal não era compatível com a criação de um método de investigação cujo funcionamento e finalidade não estavam expressos na norma em causa e concluiu pela eventual inconstitucionalidade da mesma, em virtude da violação do disposto nos artigos 18.º, n.º 2, 26.º, n.º 2 e 1.º da CRP. Assim, RAMALHO, David Silva, "O uso de *malware*…", cit., pp. 233-234

[158] RAMALHO, David Silva, *Métodos Ocultos*…, cit., pp. 345-346

[159] *Idem*

[160] *Idem*, p. 345

[161] *Idem*, p. 346

[162] *Idem*

Por sua vez, João Conde Correia concluiu igualmente pela consagração das "buscas *online*" no artigo 19.º, n.º 2 da LC, com base no elemento gramatical, ou seja, através da possibilidade de recorrer a "meios e dispositivos informáticos" quando necessário e sempre no âmbito de uma ação encoberta[163].

Por fim, Francisco Marcolino de Jesus também é defensor da previsão do uso de *malware* na LC, afirmando que "a Lei 109/2009, de 15 de setembro, ao que se crê, permite a busca *online*"[164], apesar de não esclarecer em que preceito considera estar inserido este método.

2.2. A inexistência de norma(s) habilitante(s)

Noutra perspetiva, várias são as vozes que se erguem no sentido de não existir, no nosso ordenamento jurídico, norma(s) habilitante(s) da utilização de *malware* como meio de obtenção de prova.

Relativamente à previsão do uso de *malware* no artigo 18.º da LC, David Silva Ramalho e Juliana Campos rejeitam, desde logo, este enquadramento, na medida em que tal preceito – bem como a extensão prevista no artigo 189.º do CPP – disciplinam a interceção de comunicações, isto é, a captação destas últimas entre o seu envio pelo remetente e a sua chegada ao destinatário[165]. Neste sentido, os referidos normativos excluem a recolha, oculta e remotamente, de dados armazenados e não armazenados num sistema informático[166], o que significa que o *malware* fica automaticamente fora deste quadro[167]. De facto, está em causa um método bastante mais intrusivo e muito mais abrangente que uma simples interceção,

[163] CORREIA, João Conde, "Prova digital: as leis que temos…", cit., pp. 42-43
[164] JESUS, Francisco Marcolino, *Os Meios de Obtenção da Prova em Processo Penal*, 2.ª Edição Revista, Atualizada e Ampliada, Coimbra: Almedina, 2015, p. 46
[165] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 339
[166] *Idem*
[167] Ademais, legitimar o uso de *malware* com base no artigo 18.º da LC constituiria numa inconstitucionalidade material (por violação dos artigos 18.º, n.º 2 e 34.º, n.º 4 da CRP), uma vez que a ingerência nas telecomunicações e meios de comunicação por parte das autoridades públicas só é permitida nos casos expressamente previstos na lei. Assim, CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 90-91

permitindo monitorizar toda a atividade, lícita ou ilícita, interna e externa ao sistema[168], afetando o direito à integridade e confidencialidade do sistema informático[169].

Nesta linha, também Manuel da Costa Andrade rejeita um enquadramento daquilo que designa por busca *online* no regime do artigo 18.º da LC, uma vez que aquela não configura uma intromissão nas telecomunicações, não podendo, por isso, estar abrangida nesta norma[170].

Juliana Campos rejeita também a opção de "fusão" deste meio de obtenção de prova com outros regimes, uma vez que, apesar de a utilização de *malware* também pressupor, após a sua instalação, uma apreensão dos dados que foram enviados para o OPC ou a AJ, tal parece não ser suficiente para legitimar a sua submissão ao regime das apreensões[171]. Para além disso, a autora sustenta que a apreensão pode não ter natureza oculta e o seu nível de devassa é muito inferior ao do *malware*[172].

Ainda nesta linha, no que diz respeito à fusão com o regime da recolha de voz e imagem em tempo real (artigo 6.º das Medidas de combate à criminalidade organizada[173]), a autora afasta-se, mais uma vez, desse pensamento, por entender que é um regime com requisitos muito pouco exigentes[174] para legitimar a utilização de um meio tão gravoso como este[175].

Relativamente a estas opções de fusão de regimes, David Silva Ramalho frisa que é ao legislador que compete ponderar os interesses em conflito no que concerne à restrição de direitos fundamentais aquando da consagração de cada método oculto; ademais, o intérprete não tem legitimidade para criar arbitrariamente novos meios a partir de partes de outros legalmente previstos[176]. Assim, o autor reitera que é fundamental que exista sempre uma lei,

---

[168] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 90
[169] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 341 e CORREIA, João Conde, "Prova digital: as leis que temos…", cit., p. 43
[170] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*"…, cit., pp. 160 e 168 e ANDRADE, Manuel da Costa, "Comentário ao artigo 194.º", in *Comentário Conimbricense do Código Penal*…, cit., p. 1103
[171] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 88
[172] *Idem*, p. 89
[173] Lei n.º 5/2002, de 11 de janeiro
[174] Basta-se com as suspeitas da prática de crimes do catálogo e de quem é/são o(s) seu(s) agente(s) e a respetiva necessidade para a investigação.
[175] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 99-100
[176] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 341

precisa e previsível, que regule este tipo de meios de obtenção de prova, permitindo ao visado regular a sua conduta sabendo que meios tem o Estado à disposição[177].

No que toca ao artigo 15.º da LC, apesar de admitirem algumas semelhanças em certos aspetos[178], Juliana Campos e David Silva Ramalho entendem que as diferenças entre estes dois meios de obtenção de prova prevalecem. Desde logo, o n.º 1 do referido artigo refere-se à obtenção de "dados informáticos específicos e determinados, armazenados num determinado sistema informático", o que afasta o *malware* da pesquisa, na medida em que não se pode assegurar que se vão obter dados específicos e determinados[179]. Para além disso, o excerto do preceito exclui também a obtenção de dados em tempo real e/ou não armazenados – estes que, como temos vindo a referir, são pontos característicos do método oculto em apreço – e não faz qualquer referência a uma atividade de infiltração prévia[180].

Perante isto, argumenta-se ainda que se poderia legitimar a utilização de *malware* ao abrigo do n.º 5 do artigo 15.º da LC; proposta esta que os autores referidos, assim como Sónia Fidalgo[181], também rejeitam por ser evidente que este preceito é uma mera extensão da pesquisa inicial a outro sistema e, neste sentido, tem como pressuposto uma pesquisa prévia que faria cair o caráter oculto do *malware*[182]. Face ao exposto, é notório que o *malware*, bem como todas as funcionalidades que este comporta, representam um nível de devassa muito superior ao da pesquisa informática[183], não se compatibilizando integralmente com o regime do artigo 15.º da LC.

Rita Castanheira Neves[184] sustenta que nem no artigo 15.º, nem no artigo 16.º da LC está prevista a possibilidade de se realizarem as ditas buscas *online* enquanto forma de recolha de dados informáticos sem conhecimento do visado. No primeiro caso, o preceito faz referência à presença da autoridade judiciária na diligência, o que colide com a natureza oculta do meio; no segundo caso, o n.º 7 do artigo 16.º da LC exclui a possibilidade de as

---

[177] *Idem*, p. 342
[178] Para mais desenvolvimentos sobre este ponto: CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 83-87
[179] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 86
[180] RAMALHO, David Silva, *Métodos Ocultos*…, cit., p. 342
[181] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital…", cit., p. 153
[182] *Idem*, p. 343 e CORREIA, João Conde, "Prova digital: as leis que temos…", cit., p. 42
[183] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 87
[184] NEVES, Rita Castanheira, *As ingerências nas comunicações electrónicas em processo penal. Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra: Coimbra Editora, 2011

instâncias de controlo poderem efetuar buscas sem o visado se aperceber disso. Neste sentido, a autora entende que admitir as buscas *online* consistiria numa violação do princípio da legalidade.

No mesmo sentido, Paulo Dá Mesquita[185] entende que não se confunde a utilização de *malware* com os regimes dos artigos 15.º e 16.º da LC, que correspondem, respetivamente, às pesquisas e apreensões informáticas. O autor considera que, quando existam indícios de que os dados informáticos relacionados com um crime, ou que possam servir de prova do mesmo, estejam num sistema informático, deve ser ordenada uma busca informática (artigo 174.º, n.º 1 do CPP); e que, quanto às apreensões, os pressupostos continuam a ser os previstos no artigo 178.º, n.º 1 e 3. Assim, na visão do autor, não existe aqui espaço para a instalação e utilização de *malware*.

A previsão do *malware* no regime das ações encobertas em ambiente digital (artigo 19.º, n.º 2 da LC) é também rejeitada por alguns autores.

Juliana Campos defende que estes meios de obtenção de prova não se confundem, desde logo, no que toca à sua natureza: o primeiro consiste num *software* que é instalado num sistema informático para recolher prova, tratando-se de um método passivo; por outro lado, o segundo corresponde a um funcionário de investigação criminal (ou terceiros) que, estabelecendo uma relação com o suspeito, obtém informações sobre o plano do crime, pressupondo um laço de confiança[186]. Assim, a autora entende que a expressão que sustenta tal previsão é indeterminada e imprecisa, sendo criticável à luz do princípio da determinabilidade dos atos normativos[187]. Mais, Juliana Campos salienta o facto de estarmos perante um meio com enorme alcance e elevado potencial de devassa, que restringe inúmeros direitos fundamentais, reclamando, por isso, uma lei expressa e determinada que o preveja como meio de obtenção de prova autónomo[188].

No mesmo sentido, Costa Andrade sustenta que "só uma lei expressa, clara e determinada, especificamente reportada à técnica em causa, definidora e delimitadora da

[185] MESQUITA, Paulo Dá, "Prolegómeno sobre prova electrónica e intercepção de telecomunicações…", cit., p. 115
[186] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 94-95
[187] *Idem*, p. 96
[188] *Idem*, pp. 96-97.

respetiva medida de invasividade e devassa, pode legitimar a sua utilização como meio de obtenção de prova em processo penal"[189].

Neste seguimento, também Sónia Fidalgo entende ser necessária uma lei que preveja expressamente os requisitos formais, materiais e orgânicos que tornem admissível a utilização de *malware* como meio de obtenção de prova, face à danosidade social da medida em questão[190].

Por fim, Duarte Rodrigues Nunes também considera que a norma do artigo 19.º, n.º 2 da LC não pode constituir a norma habilitante para o uso de *malware*, por entender que não foi essa a intenção do legislador ao criar a norma, mas sim a de clarificar a hipótese de serem utilizados tais meios e dispositivos informáticos no âmbito das ações encobertas *online*; além disso, o autor reitera que o preceito carece da clareza e precisão no que respeita aos pressupostos e requisitos da sua utilização, que são exigíveis tendo em conta a restrição de direitos[191].

Face a esta exposição e perante pontos de vista tão diversos, parece-nos adequado tecer alguns comentários. De facto, a utilização de *malware* como meio de obtenção de prova é uma questão controversa e que divide opiniões. De qualquer forma, do nosso ponto de vista, o *malware* tem especificidades que não permitem que este se confunda ou se equipare a outros meios de obtenção de prova já existentes e previstos no nosso ordenamento jurídico. Assim, mesmo admitindo uma aproximação em certos casos, a verdade é que seria redutor incluir este método em qualquer uma das normas que foram apontadas nesse sentido, face ao nível de devassa e de restrição dos direitos fundamentais em causa.

Neste sentido, torna-se exigível que haja uma intervenção do legislador no sentido de prever expressamente o recurso a este meio de obtenção de prova, através de uma lei clara, precisa e autónoma, que estabeleça um conjunto de requisitos apertados e excecionais para a sua admissibilidade, pois só assim poderá ser legítimo recorrer a um método que pode ser definido como o mais invasivo e restritivo de todos.

---

[189] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*"…, cit., pp. 22-23
[190] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital…", cit., p. 154
[191] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, cit., p. 372

2.3. Proposta de regime jurídico

Concluindo pela utilidade e relevância da utilização de *malware* para a descoberta da verdade, bem como pela sua não previsão como meio de obtenção de prova no nosso ordenamento jurídico, importa refletir sobre os requisitos necessários para a sua eventual admissibilidade.

Assim, passaremos a apontar os requisitos formais, materiais e orgânicos que consideramos serem fundamentais para que o *malware* seja legal e constitucionalmente admissível[192] e que o legislador deve ter em conta no momento da sua consagração, operando a concordância prática das finalidades em conflito. Neste ponto, acompanhamos Costa Andrade e a sua sistematização relativa à "teoria geral" dos métodos ocultos de obtenção de prova[193].

a) Requisitos formais

O facto de se tratar de um método altamente lesivo dos direitos fundamentais leva a uma "intransponível exigência de reserva de lei"[194], o que significa que é necessário que haja uma lei da Assembleia da República ou um decreto-lei autorizado do Governo no sentido da sua previsão, assim como a densificação do regime jurídico aplicável (cf. artigos 18.º, n.º 2 e 165.º da CRP)[195].

Não podemos esquecer que estamos perante um método oculto, o que pode potenciar a arbitrariedade da atuação estadual, sendo essencial a existência de uma lei expressa, clara e determinada que preveja este método de forma autónoma relativamente a outros[196].

Nesta linha, acompanhamos a ideia de que, nesta previsão legal, deve ser utilizada a designação "*malware*", por razões que se prendem, essencialmente, com o rigor técnico, a

[192] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 156
[193] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*"…, cit., pp. 112-119
[194] ANDRADE, Manuel da Costa, "Métodos ocultos de investigação (Plädoyer para uma teoria geral)", *Que futuro para o direito processual penal?; Simpósio em homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal Português* (coord. Mário Ferreira Monte *et. al.*), Coimbra: Coimbra Editora, 2009, p. 540
[195] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 157
[196] ANDRADE, Manuel da Costa, "Métodos ocultos de investigação…", cit., p. 540

segurança jurídica e a proteção da confiança, bem como pelo facto de existirem outros diplomas que contêm expressões não traduzidas para a língua portuguesa[197].

b) Requisitos materiais

Desde logo, é fundamental que o legislador não permita a utilização deste meio de obtenção de prova para qualquer crime, estabelecendo antes um catálogo autónomo e restrito, de crimes específicos, que deverão traduzir-se nas formas mais graves de criminalidade tendo em conta a sua lesividade[198].

Além disso, não basta que a factualidade típica seja reconduzível a um dos crimes catalogados; é necessário que se verifique, em concreto, uma suspeita fundada, isto é, deve haver indícios da prática do crime em questão e estes devem assentar em factos determinados e racionalmente sustentados[199].

Em terceiro lugar, é também exigível um catálogo de pessoas, ou seja, uma certa determinação do alvo[200], na medida em que não se deve admitir que a utilização de *malware* afete um número ilimitado de pessoas, pelo que se deve circunscrever ao suspeito, arguido e outras pessoas que, no caso, se revelem pertinentes.

No que respeita ao âmbito funcional, acresce que, em cada caso concreto, deve proceder-se à delimitação e/ou descrição da funcionalidade que vai ser utilizada, nomeadamente se o método vai ser usado para obter dados armazenados ou dados produzidos em tempo real ou se vai comportar a ativação de *hardware*. Este ponto é essencial para aferir o nível de invasão e os direitos fundamentais afetados pela medida[201].

Por sua vez, o legislador deve delimitar temporalmente a medida, estabelecendo um limite máximo para a sua execução.

---

[197] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 158
[198] *Idem*, p. 160
[199] *Idem*, p. 161
[200] *Idem*
[201] *Idem*, p. 163

Para além destes pontos, que consideramos fulcrais na previsão de um regime jurídico para a utilização de *malware* como meio de obtenção de prova, é também importante garantir o respeito por alguns princípios.

Primeiramente, no que toca ao princípio do contraditório, torna-se exigível que o juiz, no despacho de autorização: especifique o tipo de *malware* utilizado e as respetivas funcionalidades; tome medidas para garantir a integridade e autenticidade das provas; exija que se proceda à documentação do código-fonte e das mudanças nos sistemas informáticos[202].

O princípio da proporcionalidade, nas suas três vertentes[203], deve pautar o conteúdo e o regime de todos os requisitos materiais e deve ser aferido, concretamente, pelo julgador no momento de decidir pela autorização ou recusa da medida[204].

Além disso, note-se que a utilização deste método deve estar subordinada ao princípio da subsidiariedade, o que significa que este é um método de *ultima ratio*, ou seja, apenas se deve recorrer ao mesmo se não existir um meio aberto ou se nenhum outro método oculto (menos gravoso) possibilite a recolha de prova, tornando-a bastante dificultada ou até impossibilitada[205].

Por fim, não podemos deixar de referir que a "área nuclear da intimidade" está subtraída a qualquer tipo de ponderação, tendo subjacente uma "intransponível proibição de produção e valoração de provas"[206]. Estamos no âmbito do respeito pela reserva da vida privada, devendo haver uma interrupção imediata da utilização de *malware* caso surjam evidências de que as provas recolhidas contendem com esta área e, consequentemente, deve proceder-se à exclusão dos dados em questão.

c) Requisitos orgânicos

Como sabemos, a utilização de *malware*, a ter lugar, tê-lo-á na fase de inquérito, na qual se procede à investigação, e a direção desta cabe ao Ministério Público. Todavia, tendo

[202] *Idem*, pp. 164-165
[203] Adequação, necessidade e proporcionalidade em sentido estrito.
[204] CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., pp. 165-166
[205] *Idem*, p. 166
[206] *Idem*, p. 167

em conta o caráter altamente intrusivo nos direitos fundamentais, o recurso a este método deve estar sujeito a prévia autorização do juiz[207], respeitando-se assim o princípio da reserva de juiz[208]. Neste sentido, a falta de autorização do juiz conduz à ilegalidade da medida e consequente proibição de valoração dos meios de prova.

Neste âmbito, note-se que o juiz deve estender a sua intervenção ao longo da execução e utilização do *malware*, levando a cabo um acompanhamento próximo e contínuo de modo a garantir um efetivo controlo do conteúdo e dos dados acedidos, podendo fazer cessar a medida sempre que considere necessário ou justificado[209].

Em conclusão, parecem-nos ser estes os pontos essenciais para servir de base à admissibilidade da utilização de *malware* como meio de obtenção de prova no processo penal português. De facto, trata-se de um conjunto de requisitos bastante apertado, mas que nos parece efetivamente justificado tendo em conta o nível de devassa e restrição dos direitos fundamentais que está em causa com a utilização deste método.

[207] Atendendo à volatilidade da prova digital e a facilidade com que esta pode ser alterada ou eliminada, podemos admitir que, em certos casos urgentes, o método possa ser autorizado por despacho do MP, ficando sujeito a posterior validação pelo juiz.
[208] Que aqui deve ser entendida como uma reserva não só formal, mas também material, no sentido de se exigir que o juiz não tenha apenas um papel passivo, mas que tenha, efetivamente, conhecimento do método e das funcionalidades que este acarreta, de forma a garantir uma tutela preventiva e efetiva dos direitos. CAMPOS, Juliana, *O malware como meio de obtenção da prova*…, cit., p. 168
[209] *Idem*, p. 169

CAPÍTULO III

LAW IN BOOKS vs. LAW IN ACTION: A EXPERIÊNCIA AMERICANA E A EXPERIÊNCIA PORTUGUESA

No presente capítulo, dedicar-nos-emos a uma abordagem mais prática e "real" da utilização de *malware*. Assim, depois da análise que fizemos aos ordenamentos jurídicos americano e português, passaremos a expor casos recentes relativos ao uso deste meio de obtenção de prova nos EUA e em Portugal, respetivamente.

Num primeiro momento, iremos expor um caso de utilização de um tipo de *malware* como forma de recolher prova no âmbito de uma investigação criminal de enorme envergadura, impulsionada pelos EUA e que envolveu vários países e as respetivas autoridades policiais, tendo culminado numa operação de sucesso que permitiu desmantelar redes e grupos de crime organizado. Com efeito, começaremos por expor toda a "história" desta operação, começando por explicar os motivos que levaram ao surgimento da "ANOM", as suas funcionalidades, o objetivo da sua utilização, os procedimentos seguidos e os resultados alcançados.

Num segundo momento, colocaremos a hipótese de haver lugar, em Portugal, a uma operação semelhante à exposta, fazendo referência a uma notícia recente que fez "soar os alarmes" nesse sentido.

Por fim, concluiremos com uma reflexão sobre a dicotomia "*Law in books*" e "*Law in action*", no sentido de fazermos um balanço das diferenças entre aquilo que está previsto nos ordenamentos jurídicos que analisámos no capítulo anterior e a realidade da investigação criminal nas experiências apresentadas nesses mesmos países.

1. O caso americano: os dispositivos ANOM e a Operação Trojan Shield

Em março de 2018, deu-se o encerramento de uma empresa de mensagens seguras – *Phantom Secure* –, tendo deixado os agentes de crimes internacionais sem meio de comunicação e na necessidade de encontrar uma alternativa. Nesta mesma altura, o departamento do FBI (*Federal Bureau of Investigation*) de San Diego negociava com um indivíduo que se dedicava à criação de um dispositivo encriptado de "última geração" para uso por redes criminosas. Desta forma surgiu então a "ANOM": uma aplicação de mensagens para *smartphones* que garantia uma comunicação, supostamente, segura e sigilosa[210].

No fundo, falamos de uma aplicação de mensagens, instalada em *smartphones* especialmente modificados, cujo sistema operacional desativava as funções ditas normais, como chamadas de voz, *e-mail* ou serviços de localização[211]. Assim, os *smartphones* teriam de estar desbloqueados e especificamente preparados para esta aplicação[212], à qual se acedia através de um código introduzido na calculadora do respetivo telemóvel[213]. Além disso, os *smartphones* operavam numa rede fechada, uma vez que a comunicação só era possível entre utilizadores dessa mesma plataforma, isto é, entre dispositivos ANOM[214].

O uso destes dispositivos foi amplamente alargado em meados de 2019, passando a contar com centenas de utilizadores espalhados por todo o mundo, designadamente membros da máfia italiana sediados na Austrália, o crime organizado albanês, gangues de motards, redes de tráfico de droga e outros grupos de crime organizado[215]. Esta enorme difusão deveu-

[210] Autor desconhecido, "ANOM global phone sting: What we know", in *RTE News*, 08/06/2021, disponível em <https://www.rte.ie/news/2021/0608/1226913-global-crime/> (consultado a 23/11/2021)
[211] *Idem*
[212] WESTCOTT, Ben, "For years, the underworld thought its phones were safe. They fell for an encrypted app trap", in *CNN*, 09/06/2021, disponível em <https://edition.cnn.com/2021/06/08/australia/afp-fbi-anom-app-operation-ironside/index.html> (consultado a 24/11/2021)
[213] *Idem*
[214] Autor desconhecido, "ANOM: Hundreds arrested in massive global crime sting using messaging app", in *BBC*, 08/06/2021, disponível em <https://www.bbc.com/news/world-57394831> (consultado a 18/01/2022)
[215] ROBERTSON, Adi, "The FBI secretly launched an encrypted messaging system for criminals", in *The Verge*, 08/06/2021, disponível em <https://www.theverge.com/2021/6/8/22524307/anom-encrypted-messaging-fbi-europol-afp-sting-operation-trojan-shield-greenlight> (consultado a 24/11/2021) e CHAPPELL, Bill, "Drug Rings' Favorite New Encrypted Platform Had One Flaw: The FBI Controlled It", in *NPR*, 08/06/2021, disponível em <https://www.npr.org/2021/06/08/1004332551/drug-rings-platform-operation-trojan-shield-anom-operation-greenlight?t=1642543451968> (consultado a 18/01/2022)

se à sua divulgação entre os agentes de crimes, mas foi bastante potenciada por um ex-traficante de droga, Hakan Aiyk. Este, conhecido como o homem mais procurado da Austrália, foi encorajado por agentes infiltrados a usar e vender os dispositivos ANOM no mercado negro (nomeadamente, na *Dark Web*), tendo obtido enorme sucesso, visto estar sinalizado como alguém de confiança no mundo do crime[216].

Desta feita, criminosos espalhados por todo o mundo passaram a comunicar entre si através desta plataforma, que teria na base servidores *proxy* supostamente seguros e uma encriptação de "nível militar"[217].

No entanto, o serviço ANOM era, na verdade, um *malware* do tipo cavalo de troia distribuído sub-repticiamente, enquanto aplicação de mensagens encriptadas[218], pelo Departamento Federal de Investigação dos Estados Unidos (FBI – *Federal Bureau of Investigation*) e pela Polícia Federal Australiana (AFP – *Australian Federal Police*), que lhes permitia monitorizar todas as comunicações estabelecidas entre os utilizadores da aplicação sem o seu conhecimento[219]. A aplicação ANOM foi programada, secretamente, com um *backdoor*[220], permitindo o acesso e respetiva desencriptação das mensagens em tempo real[221].

No fundo, assim que os agentes de crimes utilizavam a aplicação encriptada, a polícia desencriptava as mensagens que estes enviavam e tinha acesso ao seu conteúdo[222]. Segundo consta de depoimentos, a fonte confidencial do FBI – criadora da aplicação – criou uma "chave mestra" no sistema de encriptação do dispositivo ANOM que se anexava, de forma

---

[216] TAOUK, Maryanne, "Underworld figure Hakan Ayik unwittingly helped Operation Ironside, the AFP's biggest criminal sting", in *ABC News*, 09/06/2021, disponível em <https://www.abc.net.au/news/2021-06-09/fugitive-hakan-ayik-unwittingly-helped-operation-ironside/100198164> (consultado a 24/11/2021)
[217] Autor desconhecido, "ANOM global phone sting: What we know", in *RTE News*, 08/06/2021, disponível em <https://www.rte.ie/news/2021/0608/1226913-global-crime/> (consultado a 23/11/2021)
[218] TUFFLEY, David, "AN0M: How an app to decrypt criminal messages was born 'over a few beers' with FBI", in *RNZ*, 09/06/2021, disponível em <https://www.rnz.co.nz/news/national/444358/an0m-how-an-app-to-decrypt-criminal-messages-was-born-over-a-few-beers-with-fbi> (consultado a 13/06/2022)
[219] Autor desconhecido, "Hakan Ayik: The man who accidentally helped FBI get in criminals' pockets", in *BBC*, 08/06/2021, disponível em <https://www.bbc.com/news/world-57397779> (consultado a 24/11/2021)
[220] Um *backdoor* é um *software* que defrauda o normal acesso e autenticação numa aplicação, permitindo o acesso remoto a informações privadas, sem o utilizador ter conhecimento.
[221] TUFFLEY, David, "AN0M: How an app to decrypt criminal messages was born 'over a few beers' with FBI", in *RNZ*, 09/06/2021, disponível em <https://www.rnz.co.nz/news/national/444358/an0m-how-an-app-to-decrypt-criminal-messages-was-born-over-a-few-beers-with-fbi> (consultado a 13/06/2022)
[222] *Idem*

sub-reptícia, a cada mensagem e permitia que a polícia desencriptasse e armazenasse a mensagem à medida que esta era transmitida[223].

O FBI terá pensado numa forma de todo este sistema funcionar e procurou um terceiro país que colaborasse com os EUA e a Austrália na operação. Este país – que até hoje permanece não identificado – hospedaria o servidor que desencriptava as mensagens, precisando, para isso, que a sua legislação permitisse aceitar o acesso a todas as mensagens desencriptadas para, posteriormente, serem remetidas para os servidores do FBI[224].

Assim, estabeleceu-se um acordo de cooperação internacional de forma a que toda esta estrutura funcionasse. O FBI conseguiu encontrar um terceiro país que concordou em obter uma ordem judicial para enviar as mensagens desencriptadas para um servidor onde estas seriam copiadas e enviadas ao FBI, sem acesso prévio ao seu conteúdo e sob um tratado de assistência jurídica mútua[225]. Deste modo, uma cópia de cada mensagem enviada de cada dispositivo ANOM era remetida para esse servidor do terceiro país, onde as mensagens eram armazenadas. Por sua vez, estes dados eram enviados para servidores controlados pelo FBI e toda a informação pertinente relativa a crimes era comunicada aos órgãos de polícia criminal dos países em causa[226].

Esta aplicação foi a chave do sucesso da Operação Trojan Shield[227], impulsionada pelo FBI e pela AFP e que contou com a colaboração de órgãos de polícia criminal de vários países entre 2018 e 2021. Esforços de vários anos culminaram na execução simultânea de mandados de busca em todo o mundo, no dia oito de junho de 2021[228], que tiveram como resultado a detenção de mais de 800 pessoas em 16 países, bem como a apreensão de 40

[223] BAKER, Stewart/KLEHM, Bryce, "Legal Tetris and the FBI's ANOM Program", in *Law Fare*, 22/07/2021, disponível em <https://www.lawfareblog.com/legal-tetris-and-fbis-anom-program> (consultado a 13/06/2022)
[224] *Idem*
[225] *Idem*
[226] Autor desconhecido, "FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown", in *US Department of Justice*, 08/06/2021, disponível em <https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive> (consultado a 13/06/2022)
[227] Também conhecida como Ironside ou Greenlight.
[228] Não se sabe ao certo porque terá sido esta a data escolhida, mas a especulação aponta para o facto de o mandado de acesso ao servidor expirar no dia sete de junho.

toneladas de drogas, 250 armas, 55 carros de luxo e mais de 48 milhões de dólares em moedas e criptomoedas, envolvendo mais de 9 000 polícias[229].

Descrita pela Europol como "a maior e mais sofisticada operação policial de sempre contra a comunicação encriptada"[230], teve um papel fundamental na prevenção de uma série de crimes, tendo mostrado que as autoridades têm acompanhado o constante desenvolvimento tecnológico e têm apostado na cooperação internacional[231]. Mais, graças à informação obtida através da aplicação, os órgãos de polícia criminal terão reunido inúmeras provas úteis para diversos processos por diferentes crimes[232]. Além disso, a operação permitiu ainda detetar vários casos de corrupção pública[233], tendo revelado que vários grupos criminosos estavam a ser informados sobre ações policiais[234].

De facto, o enorme sucesso, sem precedentes, da Operação Trojan Shield deve ser entendido como um aviso para todas as organizações criminosas internacionais. Um aviso no sentido de que não há garantia de segurança e sigilo nas suas comunicações, uma vez que, agora e mais do que nunca, as autoridades estão alerta, munidas de meios técnicos inovadores, de forma a trabalharem em conjunto para combater criminalidade perigosa que atravessa fronteiras internacionais[235].

---

[229] <https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication> (consultado a 13/06/2022)

[230] Jean-Philippe Lecouffe, vice-diretor de operações da Europol, segundo HADING, Luke, "Hundreds arrested in global crime sting after underworld app is hacked", in *The Guardian*, 08/06/2021, disponível em <https://www.theguardian.com/australia-news/2021/jun/08/anom-encrypted-app-fbi-afp-australia-federal-police-sting-operation-ironside-an0m> (consultado a 24/11/2021)

[231] CORDER, Mike/PERRY, Nick/SPAGAT, Elliot, "Global sting began by creating message service for crooks", in *AP news*, 09/06/2021, disponível em <https://apnews.com/article/europe-technology-a6ac691e26be2efc6e2f4a6974117536> (consultado a 23/11/2021) e ainda <<https://www.dw.com/en/trojan-shield-europol-details-massive-organized-crime-sting/a-57808917> (consultado a 18/01/2022)>

[232] Reece Kershaw, comissário da AFP, segundo CHAPPELL, Bill, "Drug Rings' Favorite New Encrypted Platform Had One Flaw: The FBI Controlled It", in *NPR*, 08/06/2021, disponível em <https://www.npr.org/2021/06/08/1004332551/drug-rings-platform-operation-trojan-shield-anom-operation-greenlight?t=1642543451968> (consultado a 18/01/2022)

[233] *Idem*

[234] HADING, Luke, "Hundreds arrested in global crime sting after underworld app is hacked", in *The Guardian*, 08/06/2021, disponível em <https://www.theguardian.com/australia-news/2021/jun/08/anom-encrypted-app-fbi-afp-australia-federal-police-sting-operation-ironside-an0m> (consultado a 24/11/2021)

[235] Suzanne Turner, agente no comando do FBI de San Diego, segundo Autor desconhecido, "FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown", in *US Department of Justice*, 08/06/2021, disponível em <https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive> (consultado a 13/06/2022)

2. O caso português: o *software* (supostamente) adquirido pela PJ e a Cellebrite

Em Portugal, "os alarmes soaram" em janeiro de 2018, quando os meios de comunicação social divulgaram uma notícia que revelava que a Polícia Judiciária iria adquirir um *software* para obter dados de telemóveis à distância[236]. De acordo com o noticiado, estaria em causa um "sistema de aquisição remota de prova digital em terminais de comunicações móveis", ou seja, um sistema informático que permitiria recolher, de forma remota, dados armazenados em telemóveis de suspeitos da prática de crimes[237].

De facto, a despesa com a aquisição deste sistema, avaliada em 2,9 milhões de euros, foi autorizada pelo Governo, constando de despacho que autorizava a repartição de encargos nos anos de 2017 e 2018, publicado em Diário da República[238]. Conforme consta da respetiva Portaria[239], a compra deste sistema tinha como objetivo dotar a PJ dos "meios técnicos adequados à promoção e reforço da prevenção e da repressão da criminalidade transnacional grave e organizada", nomeadamente "o terrorismo, o tráfico de seres humanos, o cibercrime, o tráfico de droga, o crime económico-financeiro" e fomentar a "cooperação com os restantes Estados-membros e Países Terceiros".

No entanto, se na altura a notícia prendeu as atenções e fez questionar a sua eventual ilegalidade, rapidamente o assunto foi esquecido, não tendo havido mais nenhuma divulgação sobre o mesmo ou os procedimentos que se seguiram. De facto, a notícia apenas foi divulgada em dois jornais[240] e nunca mais se falou sobre o assunto.

Tendo ou não adquirido o referido sistema, a questão que se coloca é a de saber em que termos e com base em que legislação este poderia ser utilizado. No fundo, estaria em

---

[236] 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 17/06/2022)

[237] *Idem*

[238] Diário da República n.º 2/2018, Série II de 03-01-2018, p. 164, disponível em <https://dre.pt/dre/detalhe/portaria/4-2018-114446948> (consultado a 17/06/2022)

[239] *Idem*

[240] 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 17/06/2022) e 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.sapo.pt/exameinformatica/noticias-ei/mercados/2021-05-06-pj-sef-gnr-cellebrite-portugal-codigo-azul/> (consultado a 20/06/2022)

causa a recolha de dados armazenados em equipamentos móveis, designadamente comunicações telefónicas ou através de aplicações, que seria feita "cumprindo os procedimentos legais"[241]. Porém, esta seria uma recolha à distância, levada a cabo remotamente, pelo que se poderá deduzir que seria feita sem conhecimento e consentimento do visado. Assim, estaríamos, sem sombra de dúvida, no âmbito da utilização de um *malware* como forma de obter prova perante a suspeita da prática de crime.

Face ao exposto, e tendo em conta a conclusão a que chegámos no capítulo anterior relativamente à ausência de regulação expressa deste meio de obtenção de prova no nosso ordenamento jurídico, ao confirmar-se esta aquisição, pela PJ, de um sistema de recolha de prova digital desta natureza, ter-se-ia que apurar até que ponto tal seria admissível no nosso ordenamento jurídico tal como o conhecemos até agora. Por enquanto, permanecemos na incerteza quanto à existência e/ou utilização deste tipo de métodos, em Portugal, pelas forças policiais.

Mais recentemente, em maio de 2021, os meios de comunicação social divulgaram mais uma notícia que prendeu a atenção de muitos, na qual se anunciava a compra, por parte da PJ, do SEF e da GNR[242], de um "polémico *software* israelita" para aceder a *smartphones* bloqueados[243]. Em causa estava a aquisição, por parte destes OPC, de ferramentas que permitem aceder e extrair informações de equipamentos eletrónicos, nomeadamente *smartphones* bloqueados[244].

Estas "ferramentas" são comercializadas por uma conhecida empresa israelita: a Cellebrite[245], especializada em tecnologias de investigação forense. No fundo, a empresa, que começou a comercializar as suas ferramentas para análise forense e aplicação da lei em 2007[246], disponibiliza vários meios de análise digital, mas ficou particularmente conhecida

---

[241] 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 17/06/2022)

[242] Assim como, anteriormente, a Polícia de Segurança Pública (PSP) e a Procuradoria-Geral da República (PGR).

[243] 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.sapo.pt/exameinformatica/noticias-ei/mercados/2021-05-06-pj-sef-gnr-cellebrite-portugal-codigo-azul/> (consultado a 20/06/2022)

[244] *Idem*

[245] <https://cellebrite.com> (consultado a 20/06/2022)

[246] PAGLIERY, Jose, "Cellebrite is the FBI's go-to phone hacker", in *CNN*, 01/04/2016, disponível em <https://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/index.html> (consultado a 20/06/2022)

pelos produtos que permitem aceder e extrair dados de *smartphones*[247], nomeadamente o *Universal Forensic Extraction Device* (UFED)[248].

O UFED permite aceder aos *smartphones*, mesmo que bloqueados, e permite extrair informações como mensagens, *e-mails*, registo de chamadas, fotografias, localizações e até recuperar ficheiros apagados[249].

Apesar de a notícia ter sido divulgada, de certo modo, com um tom pejorativo[250] no sentido de dar a entender que tal procedimento poderia ser ilegal, a verdade é que, após uma análise aos contornos do procedimento e à nossa legislação, facilmente concluiremos pela admissibilidade da utilização desta ferramenta por parte das entidades policiais recorrendo a algumas normas do nosso ordenamento jurídico.

Focando a nossa análise na utilização do UFED enquanto instrumento de desbloqueio de *smartphones* e acesso à informação neles contida, passaremos a expor aquele que pode e nos parece ser o seu enquadramento legal.

Desde logo, terá de haver lugar à apreensão de equipamentos eletrónicos, nomeadamente *smartphones*, no âmbito de uma investigação criminal. As apreensões são efetuadas de acordo com o disposto no artigo 178.º do CPP, incidindo sobre "instrumentos, produtos ou vantagens relacionadas com a prática de um facto ilícito típico", bem como "animais, coisas e objetos deixados pelo agente no local do crime" (cf. n.º 1 do respetivo artigo) e são autorizadas, ordenadas ou validadas por despacho da autoridade judiciária competente[251] (cf. n.º 3 do respetivo artigo).

---

[247] De realçar que esta empresa ganhou um enorme destaque quando, em 2016, alegadamente permitiu ao FBI desbloquear o iPhone de Syed Rizwan Farook – o assassino responsável pelos ataques de San Bernardino, na California, em dezembro anterior. Assim, KELION, Leo, "Israel's Cellebrite linked to FBI's iPhone hack attempt", in *BBC*, 23/03/2016, disponível em <https://www.bbc.com/news/technology-35883441> (consultado a 20/06/2022)

[248] Dispositivo universal de extração forense (tradução livre). Este está disponível em diferentes formatos: um *software* para computadores ou um *tablet* que deve ser ligado, por cabo, ao dispositivo do qual se pretender extrair a informação. Assim, <https://cellebrite.com/pt/cellebrite-ufed-pt/> (consultado a 20/06/2022)

[249] 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.sapo.pt/exameinformatica/noticias-ei/mercados/2021-05-06-pj-sef-gnr-cellebrite-portugal-codigo-azul/> (consultado a 20/06/2022) e <https://cellebrite.com/pt/cellebrite-ufed-pt/> (consultado a 20/06/2022)

[250] Desde logo por ser referir a "polémico *software* israelita".

[251] MP na fase de inquérito; juiz nas restantes fases.

Seguidamente, terá de ser ordenada a realização de pesquisa de dados informáticos nos *smartphones* apreendidos, ao abrigo do artigo 15.º da LC. Assim, quando tal se revele necessário para a produção de prova, a autoridade judiciária competente autoriza, ordena ou valida a pesquisa no respetivo sistema informático de forma a "obter dados informáticos específicos e determinados" armazenados no mesmo (cf. n.º 1 e n.º 4, alínea a) do respetivo artigo). Neste caso, tal como referido acima, pretende-se aceder a informações contidas nos *smartphones*, tais como mensagens, chamadas de voz, *e-mails*, ficheiros, fotografias, etc.

Por sua vez, haverá lugar à apreensão dos dados informáticos encontrados durante a pesquisa que se revelem necessários à produção de prova, tal como disposto no artigo 16.º da LC. Neste sentido, quando os dados encontrados durante a pesquisa aos *smartphones* se revelarem essenciais para a descoberta da verdade, a autoridade judiciária competente autoriza, ordena ou valida a apreensão dos mesmos (cf. n.º 1 e n.º 4 do respetivo artigo). No caso específico da apreensão de dados em *smartphones* através do UFED, tendencialmente estará em causa a apreensão através da realização de uma cópia dos dados (cf. n.º 7, alínea b) do respetivo artigo), que será feita em duplicado, sendo uma das cópias selada e confiada ao secretário judicial e, se for possível, os dados apreendidos devem ser certificados através de assinatura digital (cf. n.º 8 do respetivo artigo).

De realçar que sempre que, no decurso da pesquisa, forem encontrados dados suscetíveis de revelar informações pessoais ou íntimas que possam pôr em causa a privacidade do titular ou de terceiro, estes devem ser apresentados ao juiz de modo a ser feita a ponderação da sua junção aos autos (cf. artigo 16.º, n.º 3 da LC). Ademais, se forem encontradas mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, estes devem ser também apresentados ao juiz para que este decida da sua junção ou não ao processo (cf. artigo 17.º da LC e artigo 179.º do CPP).

Com efeito, após esta análise e enquadramento legal, podemos concluir que a utilização do UFED não coincide nem se confunde com a utilização de um *software* malicioso no âmbito de uma investigação criminal. Estamos perante situações substancialmente distintas, na medida em que, no primeiro caso, está em causa a apreensão de objetos que contêm informações relevantes para a produção de prova num processo, nos quais se irá proceder à pesquisa e apreensão de dados neles contidos através de um *software* que permite desbloquear o acesso a esses mesmos dados; no segundo caso, falamos da

instalação sub-reptícia e oculta de um *software* num sistema informático que se encontra na posse do seu titular/utilizador, sem o seu conhecimento ou consentimento, através do qual se procede não só à obtenção de dados armazenados no mesmo, mas também de dados não armazenados, de dados produzidos em tempo real e até à ativação de *hardware*.

Em conclusão, estes dois casos algo mediáticos mostram-nos que os meios de comunicação social portugueses têm vindo a divulgar algumas notícias que "deixam no ar" a hipótese de estarem a ser usados, pelos responsáveis pela investigação criminal, meios supostamente ilegais de obtenção de prova, sem que, porém, haja relatos ou registos de que isto efetivamente aconteça. De facto, neste segundo caso relacionado com a Cellebrite, podemos concluir que é um método bastante útil que pode colaborar na descoberta da verdade, uma vez que permite obter dados que podem ser fundamentais para a produção de prova, aos quais não seria possível aceder de outra forma.

3. Análise comparativa e reflexão final

Aqui chegados, importa refletir sobre alguns pontos, nomeadamente no que diz respeito à diferença de regimes e realidades entre o ordenamento jurídico americano e o ordenamento jurídico português, diferença esta que se traduz em experiências e resultados totalmente distintos.

Desde logo, e partindo da base fornecida pelo capítulo anterior, é evidente que não podemos comparar a realidade jurídica americana com a portuguesa no que diz respeito à consagração e ao uso de *malware* no domínio da investigação criminal. Como vimos, nos EUA, apesar de não existir uma norma expressa e específica que discipline a utilização deste meio de obtenção de prova, este é, efetivamente, utilizado pelas entidades competentes como forma de recolher prova no âmbito de um processo penal, através do recurso a normas como a *Rule 41* das FRCP ou os requisitos da Quarta Emenda à Constituição. Por outro lado, após análise das perspetivas e tentativas de enquadramento legal por parte de um variado leque de autores, parece-nos evidente que, de momento, não existe, em Portugal, uma norma capaz de servir de base ao recurso ao *malware* como meio de obtenção de prova, de forma a conseguir assegurar a necessária proteção dos direitos fundamentais do(s) visado(s).

Naturalmente, esta divergência de regimes e realidades tem repercussões ao nível dos resultados das investigações criminais. Na verdade, o facto de o uso de *malware* já fazer parte da *praxis* jurídica americana permitiu que o FBI, juntamente com a AFP, conseguisse montar uma operação de enorme envergadura, a nível mundial, que teve resultados absolutamente inéditos e contribuiu fortemente para o combate à criminalidade internacional. Mais, esta operação de sucesso serviu para mostrar que as entidades responsáveis pela investigação estão a acompanhar o progresso tecnológico e, consequentemente, que se encontram munidas dos instrumentos e das técnicas necessárias para combater uma criminalidade que se revela cada vez mais digitalizada e sofisticada. Para além disso, acreditamos que este caso contribuiu bastante para que a utilização de *malware* com estes fins comece a reunir um maior número de apoiantes, visto que este método foi a chave do sucesso da operação e, sem o recurso ao mesmo, dificilmente se conseguiria obter prova para desmantelar todas aquelas redes e grupos criminosos à escala global.

Contrariamente, na nossa perspetiva, Portugal encontra-se muito aquém de comandar ou até de poder vir a fazer parte de uma operação de tamanha dimensão, na medida em que: primeiramente, não há registos, pelo menos oficiais, da sua utilização, mesmo que com base na fusão com outros regimes ou com base na analogia, como sugerem alguns autores; em segundo lugar, a discussão e as propostas sobre o recurso a este meio de obtenção de prova são escassas e insuficientes; e, por último, até existir uma lei expressa, clara e determinada que torne o uso de *malware* admissível no âmbito da investigação criminal, não nos parece que as notícias sobre a suposta utilização deste tipo de métodos se venham a tornar numa realidade, mas antes que se mantenham como até agora: meras notícias mediáticas de base duvidosa ou incerta.

Finalmente, a forma como os EUA, na veste das autoridades competentes, lidam com a utilização do *malware* acaba por refletir, de certa forma, a dicotomia "*Law in books vs. Law in action*", na medida em que, apesar de a legislação (*Law in books*) não ter registado evoluções muito significativas quanto ao recurso a este meio, na realidade das investigações e na prática jurídica (*Law in action*), o recurso a tal método é recorrente e acompanha a evolução da sociedade e do mundo envolvente. De facto, como uma das principais características do direito é a sua perpétua mudança, o "*Law in books*" não deve permanecer imóvel, devendo sim esforçar-se continuamente para identificar e compreender as mudanças e o impacto que estas acarretam[252].

[252] HALPERIN, Jean-Louis, "Law in Books and Law in Action: The Problem of Legal Change", *Maine Law Review*, volume 64, n.º 1, artigo 4 (janeiro), 2011, p. 76, disponível em <https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1179&context=mlr> (consultado a 22/06/2022)

CONCLUSÃO

Os dias de hoje são marcados pelo universo digital e pelas sucessivas novidades tecnológicas. A vida, individual e em sociedade, tornou-se largamente dependente das novas tecnologias em todos os seus setores e vertentes.

Com efeito, a criminalidade não fugiu desta realidade e, atualmente, o ambiente digital é palco de um número cada vez maior de crimes. Na verdade, falamos de crimes que são pensados ao pormenor e que são praticados com recurso a técnicas sofisticadas e praticamente imunes aos meios de obtenção de prova tradicionais. Neste sentido, a investigação criminal depara-se com uma nova realidade: a obtenção de prova torna-se cada vez mais complexa, sendo cada vez mais difícil e, por vezes, mesmo impossível, provar certos factos devido ao incremento das denominadas "medidas anti-forenses".

Posto isto, urge a adoção de um método capaz de enfrentar todas estas barreiras, que garanta a eficácia e eficiência da ação penal: assim chegámos à conclusão da utilidade e relevância prática do *malware* como meio de obtenção de prova. Este consiste num programa informático que se aproveita de uma vulnerabilidade de um sistema informático para ser instalado no mesmo, local ou remotamente, sem o conhecimento e consentimento esclarecido do utilizador. Após esta instalação, este *software* malicioso pode pôr em prática um variadíssimo leque de funcionalidades que permitirão às autoridades competentes recolher provas da prática de crimes – provas estas que, face aos entraves anteriormente expostos, seriam, de outra forma, muito difíceis ou impossíveis de obter.

Neste seguimento, é evidente que estamos perante um método oculto de investigação, o que, inevitavelmente, nos remete para um conflito entre as finalidades do processo penal: por um lado, proclama-se a sua admissibilidade em nome da descoberta da verdade material e da realização da justiça; por outro, rejeita-se a sua adoção devido à enorme restrição de direitos fundamentais que está em causa e que reclamam proteção por parte do Estado. A solução para este problema está em encontrar um ponto de equilíbrio que permita harmonizar as finalidades em conflito, tal como nos ensina Figueiredo Dias. Assim, caberá sempre ao legislador, e nunca ao intérprete ou aplicador, encontrar este ponto de concordância prática que permita o recurso a um método deste tipo.

Após estas considerações, procedemos a uma análise sobre a consagração e o uso deste meio de obtenção de prova noutros ordenamentos jurídicos (tais como o espanhol, o italiano e o alemão), com especial destaque para o direito norte-americano, assim como partimos para uma análise mais profunda à lei portuguesa com o intuito de perceber se o *malware* se encontra ou não previsto de alguma forma no nosso ordenamento jurídico. Neste último ponto, e após uma avaliação dos prós e contras apresentados por um vasto leque de autores, parece claro que o *malware* não está – nem poderia estar, a nosso ver, nestes termos – consagrado no ordenamento jurídico português, pelo que passamos para a apresentação de uma proposta do regime jurídico que nos parece ser o mais adequado e respeitador dos direitos fundamentais, expondo um conjunto de requisitos formais, materiais e orgânicos que jamais poderão ser descurados aquando da adoção de um método restritivo e invasivo como este.

Por fim, a exposição mais detalhada destes dois ordenamentos jurídicos – americano e português – serviu de base e fio condutor a uma análise mais prática e reflexiva que levamos a cabo no último capítulo e que pretende mostrar o atual estado da arte no que diz respeito à utilização do *malware* como meio de obtenção de prova. Assim, procedemos a uma análise comparativa entre o recurso, frequente e bem-sucedido, a este método por parte das autoridades americanas e a especulação sobre a (não) utilização do mesmo por parte das autoridades portuguesas.

Em suma, e numa perspetiva mais pessoal, cremos que o fundamental é encontrar o referido ponto de equilíbrio. É inevitável que o mundo avance a nível tecnológico e este avanço tem, necessariamente, de ser acompanhado por uma evolução do Direito e do Processo Penal. O aparecimento de novas práticas e novas técnicas no mundo do crime exige respostas mais eficazes e rigorosas por parte das autoridades competentes, sendo certo que isto implicará uma maior devassa da vida de cada um de nós. Assim, cabe ao legislador contrabalançar esta invasão e restrição de direitos com medidas específicas e exigentes que apenas admitam a adoção de tal método quando cumpridos cada um dos requisitos que a justifiquem. Encontrado este ponto de equilíbrio e transposto para uma lei expressa, clara e determinada, acreditamos que a consagração e utilização do *malware* como meio de obtenção de prova pode consistir numa mais-valia para os ordenamentos jurídicos dos diversos países, contribuindo para o sucesso das investigações criminais e para uma maior cooperação internacional face ao fenómeno da globalização deste tipo de criminalidade.

BIBLIOGRAFIA

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

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: Coimbra Editora, 2009

_____, "Comentário ao artigo 194.º", in *Comentário Conimbricense do Código Penal: Parte Especial* (dir. Jorge Figueiredo Dias), T. I, 2.ª Edição, Coimbra: Coimbra Editora, 2012

_____, "Métodos ocultos de investigação (Plädoyer para uma teoria geral)", *Que futuro para o direito processual penal?; Simpósio em homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal Português* (coord. Mário Ferreira Monte *et. al*.), Coimbra: Coimbra Editora, 2009

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

Autor desconhecido, "ANOM global phone sting: What we know", in *RTE News*, 08/06/2021, disponível em <https://www.rte.ie/news/2021/0608/1226913-global-crime/> (consultado a 23/11/2021)

Autor desconhecido, "ANOM: Hundreds arrested in massive global crime sting using messaging app", in *BBC*, 08/06/2021, disponível em <https://www.bbc.com/news/world-57394831> (consultado a 18/01/2022)

Autor desconhecido, "Anom: The app at the heart of the FBI's major transnational sting", in *NZ Herald*, 08/06/2021, disponível em <https://www.nzherald.co.nz/nz/anom-the-app-at-the-heart-of-the-fbis-major-transnational-sting/HUPSM4FPQT2KZCBSVAUINWA2GE/> (consultado a 18/01/2022)

Autor desconhecido, "FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown", in *US Department of Justice*, 08/06/2021, disponível em <https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive> (consultado a 13/06/2022)

Autor desconhecido, "Hakan Ayik: The man who accidentally helped FBI get in criminals' pockets", in *BBC*, 08/06/2021, disponível em <https://www.bbc.com/news/world-57397779> (consultado a 24/11/2021)

Autor desconhecido, "Protecting Pivacy Under the Fourth Amendment", *The Yale Law Journal*, n.º 2, vol. 91, 1981, disponível em <https://openyls.law.yale.edu/handle/20.500.13051/16120> (consultado a 16/06/2022)

BAKER, Stewart/KLEHM, Bryce, "Legal Tetris and the FBI's ANOM Program", in *Law Fare*, 22/07/2021, disponível em <https://www.lawfareblog.com/legal-tetris-and-fbis-anom-program> (consultado a 13/06/2022)

CAMPOS, Juliana, *O malware como meio de obtenção da prova em processo penal*, Coimbra: Almedina, 2021

CHAPPELL, Bill, "Drug Rings' Favorite New Encrypted Platform Had One Flaw: The FBI Controlled It", in *NPR*, 08/06/2021, disponível em <https://www.npr.org/2021/06/08/1004332551/drug-rings-platform-operation-trojan-shield-anom-operation-greenlight?t=1642543451968> (consultado a 18/01/2022)

CORDER, Mike/PERRY, Nick/SPAGAT, Elliot, "Global sting began by creating message service for crooks", in *AP news*, 09/06/2021, disponível em <https://apnews.com/article/europe-technology-a6ac691e26be2efc6e2f4a6974117536> (consultado a 23/11/2021)

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

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

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

HADING, Luke, "Hundreds arrested in global crime sting after underworld app is hacked", in *The Guardian*, 08/06/2021, disponível em <https://www.theguardian.com/australia-

news/2021/jun/08/anom-encrypted-app-fbi-afp-australia-federal-police-sting-operation-ironside-an0m> (consultado a 24/11/2021)

HALPERIN, Jean-Louis, "Law in Books and Law in Action: The Problem of Legal Change", *Maine Law Review*, volume 64, n.º 1, artigo 4 (janeiro), 2011, disponível em <https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1179&context=mlr> (consultado a 22/06/2022)

JESUS, Francisco Marcolino, *Os Meios de Obtenção da Prova em Processo Penal*, 2.ª Edição Revista, Atualizada e Ampliada, Coimbra: Almedina, 2015

KELION, Leo, "Israel's Cellebrite linked to FBI's iPhone hack attempt", in *BBC*, 23/03/2016, disponível em <https://www.bbc.com/news/technology-35883441> (consultado a 20/06/2022)

MESQUITA, Paulo Dá, "Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal português – o Código e a Lei do Cibercrime", *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Coimbra Editora, 2010

MILITÃO, Renato Lopes, "A propósito da prova digital no processo penal", *Revista da Ordem dos Advogados*, volume I, ano 72, 2012

NEVES, Rita Castanheira, *As ingerências nas comunicações electrónicas em processo penal. Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra: Coimbra Editora, 2011

NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, 2.ª Edição Revista e Atualizada, Coimbra: Gestlegal, 2021

PAGLIERY, Jose, "Cellebrite is the FBI's go-to phone hacker", in *CNN*, 01/04/2016, disponível em <https://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/index.html> (consultado a 20/06/2022)

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.sapo.pt/exameinformatica/noticias-ei/mercados/2021-05-06-pj-sef-gnr-cellebrite-portugal-codigo-azul/> (consultado a 20/06/2022)

QUINLAN, Sayako/WILSON, Andi, "*A Brief History of Law Enforcement Hacking in the United States*", 2016, disponível em <https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf> (consultado a 15/06/2022)

RAMALHO, David Silva, "A investigação criminal na Dark Web", *Revista de Concorrência e Regulação*, ano IV, n.º 14/15 (abril/setembro), 2013

_____, *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 (outubro/dezembro), 2013

ROBERTSON, Adi, "The FBI secretly launched an encrypted messaging system for criminals", in *The Verge*, 08/06/2021, disponível em <https://www.theverge.com/2021/6/8/22524307/anom-encrypted-messaging-fbi-europol-afp-sting-operation-trojan-shield-greenlight> (consultado a 24/11/2021)

RODRIGUES, Anabela Miranda, "A defesa do arguido: uma garantia constitucional em perigo no «admirável mundo novo»", *Revista Portuguesa de Ciência Criminal*, ano 12, n.º 4 (outubro/dezembro), 2002

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 17/06/2022)

SOUSA, Susana Aires de, "Ações encobertas (e outras figuras próximas) na investigação da criminalidade económico-financeira", *Julgar*, n.º 38 (maio/agosto), 2019

_____, "*Agent provocateur* e meios enganosos de prova. Algumas reflexões", *Separata de Liber Discipulorum para Jorge de Figueiredo Dias*, Coimbra: Coimbra Editora, 2003

TAOUK, Maryanne, "Underworld figure Hakan Ayik unwittingly helped Operation Ironside, the AFP's biggest criminal sting", in *ABC News*, 09/06/2021, disponível em <https://www.abc.net.au/news/2021-06-09/fugitive-hakan-ayik-unwittingly-helped-operation-ironside/100198164> (consultado a 24/11/2021)

THOMPSON II, Richard M., "Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure", *Congressional Research Service*, 8 de setembro de 2016, disponível em <https://fas.org/sgp/crs/misc/R44547.pdf> (consultado a 15/06/2022)

TUFFLEY, David, "AN0M: How an app to decrypt criminal messages was born 'over a few beers' with FBI", in *RNZ*, 09/06/2021, disponível em <https://www.rnz.co.nz/news/national/444358/an0m-how-an-app-to-decrypt-criminal-messages-was-born-over-a-few-beers-with-fbi> (consultado a 13/06/2022)

VENÂNCIO, Pedro Dias, *Lei do Cibercrime: anotada e comentada*, Coimbra: Coimbra Editora, 2011

VERDELHO, Pedro, "A nova Lei do Cibercrime", *Scientia Ivridica – Revista de Direito Comparado Português e Brasileiro*, 320 (outubro/dezembro), 2009

WESTCOTT, Ben, "For years, the underworld thought its phones were safe. They fell for an encrypted app trap", in *CNN*, 09/06/2021, disponível em <https://edition.cnn.com/2021/06/08/australia/afp-fbi-anom-app-operation-ironside/index.html> (consultado a 24/11/2021)

Outros links consultados

<https://debates.parlamento.pt/catalogo/r3/dar/01/10/04/102/2009-07-09/40?pgs=40-45&org=PLC&plcdf=true> (consultado a 09/05/2022)

<https://www.justice.gov/archives/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation> (consultado a 15/06/2022)

<https://www.wired.co.uk/article/operation-torpedo-fbi> (consultado a 15/06/2022)

<https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv> (consultado a 16/06/2022)

<https://www.dw.com/en/trojan-shield-europol-details-massive-organized-crime-sting/a-57808917> (consultado a 18/01/2022)

<https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication> (consultado a 13/06/2022)

<https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-smashes-organised-crime> (consultado a 13/06/2022)

<https://dre.pt/dre/detalhe/portaria/4-2018-114446948> (consultado a 17/06/2022)

<https://cellebrite.com> (consultado a 20/06/2022)

Jurisprudência

Portugal:

Tribunal Constitucional

Acórdão do TC n.º 687/2021, disponível em <https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html> (consultado a 30/11/2021)

EUA:

Supreme Court

Olmstead v. United States (1928), disponível em <https://supreme.justia.com/cases/federal/us/277/438/> (consultado a 16/06/2022)

Goldman v. United States (1942), disponível em <https://supreme.justia.com/cases/federal/us/316/129/> (consultado a 16/06/2022)

Katz v. United States (1967), disponível em <https://supreme.justia.com/cases/federal/us/389/347/> (consultado a 16/06/2022)

Tribunal Distrital do Sul do Texas

_____Divisão de Houston, de 22/04/2013 (Caso H-13-234M), disponível em <https://pt.scribd.com/doc/137842124/Texas-Order-Denying-Warrant> (consultado a 15/06/2022)