INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

A utilização de *Malware* pelos Agentes Encobertos no âmbito da Investigação Criminal na *DarkWeb*

Gabriel Caliça da Silva

Dissertação de Mestrado em Ciências Policiais
Área de especialização em Criminologia e Investigação Criminal

Orientação Científica:

Prof. Doutor José Fernandes Fontes
Castelo Branco

Academia Militar

Coorientação Científica:

Mestre Nuno Ricardo Pica dos Santos

Instituto Superior de Ciências Policiais e Segurança Interna

Lisboa, outubro 2023

Agradecimentos

Os agradecimentos que serão feitos, embora curtos, serão sentidos.
Começar por agradecer ao Instituto Superior de Ciências Policiais e Segurança Interna, em concreto, todos os senhores doutores professores que estiveram presentes no primeiro ano de mestrado e que me proporcionaram as bases, os conhecimentos para que pudesse elaborar a presente dissertação de mestrado. A ajuda destas pessoas foi importantíssima.

Um especial agradecimento ao meu orientador, o prof. dr. José Fernandes Fontes Castelo Branco, e ao coorientador, mestre Nuno Ricardo Pica dos Santos, que embora não tenha solicitado muito a ajuda dos mesmos, sempre que tive alguma dúvida ou dificuldade prontamente se mostravam disponíveis para me ajudar, com o intuito de atingir o sucesso neste projeto.

E finalmente a toda a minha família que, nos bons e maus momentos, estiveram sempre presentes e me deram forças para continuar a realizar a presente dissertação de mestrado. Em especial, à minha mãe, o meu muro, a minha fortaleza, o meu porto de abrigo. Sem ela seria impensável concluir este trabalho. Sempre insistente e pendente do andamento da elaboração da dissertação de mestrado.

Um muito obrigado, a todos os envolvidos direta ou indiretamente neste processo.

Siglas e Abreviaturas

Ac. – Acórdão

AE – Agente Encoberto/Ação Encoberta

AJ – Autoridade Judiciária

Art(s) – Artigo(s)

Cf. – conforme

CP – Código Penal

CPP – Código Processo Penal

CRP – Constituição da República Portuguesa

DLG – Direitos Liberdades e Garantias

DPP – Direito Processual Penal

EU – União Europeia

FBI – *Federal Bureau of Investigations*

I.E. – isto é

JIC – Juiz de Instrução Criminal

LC – Lei do Cibercrime

Mm. – Meritíssimo Juiz

MP – Ministério Público

Nº(s) – Número(s)

OPC – Órgão de Polícia Criminal

PJ – Polícia Judiciária

RJAE – Regime Jurídico das Ações Encobertas

STJ – Supremo Tribunal de Justiça

TC – Tribunal Constitucional

TRL – Tribunal da Relação de Lisboa

TRP – Tribunal da Relação do Porto

V.G. – *verbi gratia* (por exemplo)

Resumo

É preciso ter em atenção que a presente dissertação de mestrado, tem como pressuposto o facto do *Malware*, atualmente, não puder ser aplicado pelos agentes encobertos, nem de outro modo, durante a investigação criminal. Esta possibilidade não é equacionada visto que no nosso ordenamento jurídico não existe nenhuma abertura para que se possa utilizar o *Malware* como meio de obtenção de prova, quer seja pela interpretação de normas, nomeadamente, aquelas que encontramos na LC, quer pela aplicação expressa do *Malware*, algo que não existe, nos dias de hoje.

A partir desta ideia, entendemos que deve ser feita uma alteração legislativa, no futuro próximo, tal como será elencado num dos capítulos e ainda a possibilidade de conciliar dois meios ocultos de obtenção de prova, como é o caso das ações encobertas em ambiente digital e o *Malware*.

Palavras-chave: *Malware*; Agente Encoberto; Meio Oculto de Obtenção de Prova; Lei do Cibercrime; Ambiente Digital; *DarkWeb*; Investigação Criminal.

Abstract

It should be noted that this master's dissertation is based on the assumption that *Malware* cannot currently be used by undercover agents or in any other way during a criminal investigation. This possibility is not considered because in our legal system there is no opening for *Malware* to be used as a covert means of obtaining evidence, either through the interpretation of existing rules, namely those found in the LC, or through the express application of *Malware*, something that does not exist to this day.

Based on this basic idea, we believe that a legislative change should be made in the near future, as will be listed in one of the chapters, as well as the possibility of reconciling two hidden means of obtaining evidence, such as covert actions in the digital environment and *Malware*.

Keywords: *Malware*; Covert Agent; Hidden Means of Obtaining Evidence; Cybercrime Law; Digital Environment; DarkWeb; Criminal Investigation.

Índice

Introdução

A presente dissertação de mestrado tem como tema principal a utilização de *Malware* pelo agente encoberto durante uma investigação criminal na *DarkWeb*. Este tema, divide-se em dois grandes temas, distintos quanto ao conteúdo. Por um lado, o *Malware* e a sua relevância no âmbito dos meios de obtenção de prova, e por outro lado, as AE e o destaque dado ao seu regime jurídico em ambiente digital contrapondo-o com o regime jurídico em vigor das AE em ambiente físico. A escolha deste tema, prende-se, não só, pelo facto de ser um assunto pouco desenvolvido no nosso ordenamento jurídico, mas também porque atualmente esta realidade tem grande impacto na investigação criminal e a tendência é verificar-se um crescimento constante, sem sinais de abrandamento. Relativamente ao *Malware*, é um tema em constante desenvolvimento porque, atualmente, vivemos numa sociedade em que a internet e as novas tecnologias predominam e uma elevada percentagem da criminalidade, nos dias de hoje, é executada com recurso aos meios tecnológicos.

Nos últimos anos a cibercriminalidade tem verificado, um aumento exponencial face ao desenvolvimento tecnológico que se verificou e que continuará a verificar-se, por exemplo, através da inteligência artificial. Em termos estatísticos[1], a título de curiosidade, no nosso país entre março e maio de 2020, em período de pandemia covid-19, registaram-se 544 denúncias pelo MP, em relação à cibercriminalidade, das quais apenas 138 foram reencaminhadas para inquérito. No ano seguinte[2], no primeiro trimestre o n.º de denúncias aumentou para 594, das quais 113 foram reencaminhas para inquérito. Estes dados são demonstrativos desta problemática no nosso ordenamento jurídico e demonstram a dificuldade que o OPC tem na investigação dos mesmos por falta de meios à sua disposição para os combater.

[1] Com base na Informação recolhida em: Cibercrime em 2020 – denúncias recebidas | GabinetedeCibercrime (ministeriopublico.pt).

[2] Atendendo à Informação recolhida em: Cibercrime em 2021 (1º Semestre) – denúnciasrecebidas | GabinetedeCibercrime (ministeriopublico.pt).

A constante evolução e proliferação dos sistemas informáticos e a modernização dos dispositivos eletrónicos estimularam o surgimento e o desenvolvimento de novos ilícitos criminais. Inclusivamente, os crimes que anteriormente eram perpetrados exclusivamente em ambiente físico, onde estabeleciam contactos constantes e presenciais entre os suspeitos envolvidos, começaram a ser executados maioritariamente através de um dispositivo eletrónico diminuindo assim, o risco de captura por parte do OPC, garantindo também o seu anonimato e a segurança não só para si como para as pessoas que o rodeiam. A criminalidade "tradicional", nomeadamente, o tráfico de seres humanos, a pedofilia, a exploração e tráfico de menores, beneficiou muito com a modernização da sociedade e com o desenvolvimento tecnológico permitiu-lhes adotar novas formas de atuação que fossem mais informatizadas acompanhando o desenvolvimento da informática e dos dispositivos eletrónicos.

No caso da criminalidade que envolve transações comerciais, nomeadamente, o tráfico de estupefacientes ou o tráfico de droga, desenvolveram-se de tal modo que atualmente as partes envolvidas no negócio não tem de se conhecer pessoalmente podendo concluir o negócio na internet através de um dispositivo eletrónico em que o vendedor envia o produto para uma determinada morada e o comprador realiza o pagamento, mais frequentemente, em *bitcoin*, uma modalidade de criptomoedas. Os criminosos cada vez mais, tem tendência para abdicar dos métodos "tradicionais", adaptando-se a esta nova realidade, e utilizam novas possibilidades que estão à sua disposição e que são altamente vantajosas para a concretização dos seus objetivos, porque não só lhes permitem praticar ilícitos criminais sem deslocarem-se da sua área geográfica o que, por sua vez, dificulta a atuação das autoridades policiais no âmbito da investigação criminal. Em contraposição, aumentou a dificuldade do OPC em identificar o ilícito criminoso, bem como, o(s) agente(s) envolvido(s), ou seja, se utilizássemos uma balança, num prato estava a capacidade que os criminosos têm de se adaptar facilmente aos constantes desenvolvimentos e modificando o seu *modus operandi*. No outro prato da balança colocaríamos a dificuldade sentida pelo OPC no âmbito da investigação criminal de combater a cibercriminalidade, como já vimos.

O que também veio dificultar o modo de atuação das autoridades policiais e judiciárias no âmbito da investigação criminal foi a diversidade de medidas anti-forenses[3], analisadas mais em detalhe noutro momento. Estas medidas permitem manter o anonimato dos seus utilizadores, protegendo-os, mas não implica necessariamente, o cometimentode ilícitos criminais.

São várias as atividades criminosas desenvolvidas pelos seus agentes através da utilização do *Malware* expondo os dados confidenciais de terceiros ou de pessoas coletivas, com o objetivo de chantageá-los a troco de avolumadas quantias, ou *bitcoin,* para reaverem esses mesmos dados, ou informações sigilosas. Neste sentido, a possível utilização deste instrumento como meio oculto de obtenção de prova, pese embora a sua danosidade, irá permitir um combate mais eficaz perante a criminalidade mais gravosa visto que os meios de obtenção de prova atuais, são insuficientes no combate a esta criminalidade. Não só Portugal, mas também os outros Estados, tem de ter a capacidade de combater os desafios impostos pelo constante desenvolvimento da sociedade através da implementação de novos meios de obtenção de prova, com o intuito de garantir a segurança dos seuscidadãos e proteger os DLG.

Nos dias de hoje, apreender um computador ou outro dispositivo eletrónico não é garantia de conclusão da investigação criminal ou de deter o suspeito da prática do crime, porque o conteúdo pode estar completamente encriptado e nenhum dos tradicionais meios de obtenção de prova tem a capacidade de os desencriptar, e aquela apreensão mostra-se inútil. O mesmo sucede se olharmos para a interceção de comunicações, se estas estiverem sido encriptadas pelos seus utilizadores torna-se impossível aceder ao seu conteúdo, sendo totalmente irrelevante se a comunicação foi ou não apreendida, porque não conseguem solucionar o problema. É necessário ultrapassar as limitações demonstradas pelos meios de obtenção de prova “tradicionais”, e

[3] Visto que “podem ser utilizadas como ferramentas de segurança contra crimes que correm por meio de sistemas informáticos, protegendo o usuário comum da criminalidade em ambiente digital” *in* RIBOLI, EDUARDO BOLSONI. *A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a intercetação de comunicações em massa e os softwares de espionagem.* P.3. Galileu – Revista de Direito e Economia, volume XIX, 1 de julho a 31 de dezembro de 2018.

desenvolver novos meios de obtenção de prova na investigação criminal que permitam recolher dados, informações mais rápida e eficazmente, e até mesmo aceder aqueles dados que eventualmente nunca se teria acesso utilizando os meios de obtenção de prova"tradicionais".

Em virtude da constante evolução informática e a aprendizagem de novas tecnologias por parte dos criminosos, e da necessidade de se desenvolver novos meios mais eficazes no combate à cibercriminalidade e outras formas de criminalidade mais gravosas, que este conceito adquire ainda mais força e importância no âmbito do DPP no nosso ordenamento jurídico porque no âmbito da investigação criminal permitem a recolha de prova, acedendo a dados que dificilmente poderiam ser obtidos se continuássemos a utilizar os meios "tradicionais", "abertos" de obtenção de prova. Estes meios com o passar do tempo revelam a sua inadequação, ineficácia, quando confrontamos com a cibercriminalidade ou com qualquer outra forma de crime cuja atividade é exercida em ambiente digital, por exemplo se os dados que queremos recolher estiverem encriptados e armazenados nos sistemas informáticos dificilmente o OPC conseguiriam extrair o conteúdo dos mesmos.

Neste sentido, é importante realçar que as duas temáticas que sustentam todo este estudo, estão inseridos no DPP português, e englobam o conceito de meios ocultos de obtenção de prova. Este conceito pode ser definido[4] com a seguinte expressão: "aqueles métodos que representam uma intromissão nos processos de ação, interação, informação e comunicação das pessoas concretamente visadas, sem que as mesmas disso tenham consciência, conhecimento ou disso sequer se apercebam". Por outras palavras, trata-se de um conjunto de meios de obtenção de prova que pela sua natureza podem ser autorizados pela autoridade judiciária sem que antes se dê conhecimento ao visado, pois esse conhecimento poderia frustrar a intenção de o utilizar, logo durante o período em que esta a ser utilizado este meio de

[4] *In* RODRIGUES, BENJAMIM SILVA. *Da prova penal. tomo II Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*. P. 37. 1ªedição, Editora Rei dos Livros,Lisboa, 2010.

obtenção de prova o suspeito age com tamanha normalidade porque desconhece a realidade dos factos e só terá esse conhecimento num momento posterior. A este respeito importa referir que no ordenamento jurídico português, esta modalidade de meios de obtenção de prova esta regulada num único diploma, como se verifica, com os meios "abertos" ou "tradicionais" de obtenção de prova que se encontram regulados no CPP, mas não na sua totalidade, também podem ser encontrados em legislação avulsa.

Os meios ocultos de obtenção de prova encontram-se em legislação avulsa[5], nomeadamente, a lei n.º 101/2001[6], a lei n.º 5/2002[7], a lei n.º 109/2009[8], entre outras. A este respeito COSTA ANDRADE[9], não concorda com a opção do legislador visto que o mesmo em 2007, ano em que o CPP foi revisto, não deu o devido destaque aos meios de obtenção de prova considerando que a melhor solução seria a introdução destes métodos no próprio CPP, como foi o entendimento do legislador alemão, no respetivo ordenamento jurídico. Esta era a melhor situação possível porque permitia a criação de um regime dedicado a estes meios no âmbito das restrições dos DLG no âmbito da investigação criminal.

Deste modo o que irá acontecer, é que os suspeitos sem saberem estão a contribuir[10] para a produção de prova contra si mesmos. No âmbito deste conceito incluem-se, as escutas telefónicas, a intromissão em correio eletrónico, a localização GPS, videovigilância e, mais importante para efeitos do presente estudo, o recurso às AE. No seguimento desta lógica é possível admitir que a utilização de *Malware* como meio de obtenção de prova será possível sempre no âmbito dos meios ocultos de obtenção de prova, devido ao seu carater excecional.

---

[5] Cf. LIMA, ANA CATARINA RATO. *A figura do Agente Provocador e consequências da sua atuação em matéria de prova.* Mestrado em Direito e Prática Jurídica com especialidade em Ciências Jurídico-Forenses. Lisboa, 2020.

[6] Consagra o Regime Jurídico das Ações Encobertas para fins de Prevenção e Investigação Criminal.

[7] Estabelece as Medidas de combate à criminalidade organizada, onde consta como meio de obtenção de prova o registo de voz e de imagem, no art.º da presente lei.

[8] Prevê a Lei do Cibercrime, onde encontramos múltiplos meios de obtenção de prova, entre os arts.º 11.º a 19.º.

[9] *In* OLIVEIRA, JOÃO COSME TEIXEIRA DE. *Investigação no crime organizado: métodos ocultos de investigação a partir da atuação do agente infiltrado.* P.24. Dissertação de Mestrado na Universidade Lusíada do Porto, 2015.

[10] *In* 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.* Pp. 105-106. Coimbra Editora, 2009.

Regra Geral, os meios ocultos de obtenção de prova, são considerados métodos relativamente proibidos de prova com base no disposto no n.º 3 do art.º 126.º do CPP conjugado com o art.º 125.º do mesmo diploma e com outros art.º da CRP, nomeadamenteo n.º 2 e 3 do art.º 18.º e o n.º 8 do art.º 32.º.

Relativamente ao *Malware* e às AE, realidades que importam neste contexto, enquanto meios ocultos de obtenção de prova, provocam a restrição de vários DLG, nomeadamente, o direito à intimidade da vida privada, a inviolabilidade do domicílio, bem como a inviolabilidade de correspondência. Mas também podem, em certa medida, afetar direitos processuais do arguido. Assim sendo, e tendo em consideração o carater excecional destas duas realidades é fundamental que a sua aplicação esteja devidamente consagrada em legislação, quer seja no CPP, quer seja na LC, ou em lei avulsa própria.

Neste contexto, COSTA ANDRADE[11], afirma que "o recurso a um novo meio técnico de prova, oculto ou invasivo, só é possível depois de haver uma prévia e explicita legitimação legal, sendo ainda necessário que a intromissão legalmente autorizada esteja finalisticamente vinculada, obrigando-se o legislador a determinar de forma precisa o fim da recolha de uma dada informação". De certo modo, esta exigência já existe em relação às AE. Mas, como veremos, se analisarmos o seu regime em ambiente digital o problema agrava-se, porque o seu regime jurídico é praticamente inexistente, visto que o art.º 19.º da LC remete todo o regime jurídico para o disposto na RJAE.

Em relação ao *Malware* a questão é ainda mais gritante, visto que não existe nenhuma previsão legal e, por isso mesmo, existem autores na nossa doutrina que afirmam a sua aplicação através da subsunção de artigos consagrados na LC. Toda esta situação é bem demonstrativa da escassez de previsão legal, no que concerne à utilização de meios de obtenção de prova em ambiente digital, mais concretamente no combate à criminalidade na DarkWeb.

[11] Cf. NEVES, RITA CASTANHEIRA. *As ingerências nas comunicações eletrónicas em processo penal: Natureza e respetivo regime jurídico do correio eletrónico enquanto meio deobtenção de prova.* p. 56. Coimbra Editora, 2011.

Uma possível alteração legislativa, com a implementação do recurso ao *Malware* como novo meio oculto de obtenção de prova permitiria ao OPC, após requerimento apresentado pelo MP e devidamente autorizado pelo JIC, socorrerem-se a novos meios mais eficazes, que até então eram proibidos, e assim combater a cibercriminalidade e outras formas de criminalidade mais gravosas.

Posto isto, e com base no tema principal da presente dissertação de mestrado, a pergunta de investigação que queremos ver esclarecida, é a compatibilidade, ou não, do ponto de vista teórico, do *Malware* e do AE no âmbito de uma investigação criminal, ou seja, pretendemos verificar a possibilidade de estas duas realidades serem utilizadas em simultâneo durante uma investigação criminal. Todavia existem outras questões que pretendemos ver respondidas, v.g., se o nosso ordenamento jurídico, atualmente, regula como meio de obtenção de prova o *Malware*; - o facto de não existir norma habilitante impede a utilização deste instrumento ou podemos subsumi-lo noutra disposição legal; - se existem, ou não, diferenças entre o regime jurídico das AE em ambiente físico e o regime jurídicodas AE em ambiente digital.

Relativamente a estas questões, nós estabelecemos os seguintes objetivos, entre eles: analisar a atual LC e sugerir nova alteração legislativa sempre que se mostra necessário. Assim conseguiremos ampliar o catálogo de todos os meios de obtenção de prova, introduzindo um novo instrumento no catálogo, o *Malware* com base nos princípios e direitos constitucionais, e processuais, estabelecidos no nosso ordenamento jurídico. Ainda, compreender os aspetos positivos e negativos da utilização do *Malware* no DPP. É também necessário analisar o regime jurídico das Ações Encobertas em sentido lato, pelo que também carece de analise o regime jurídico das Ações Encobertas em ambiente digital, e finalmente verificar, teoricamente, a exequibilidade prática dos AE puderem utilizar este novo instrumento.

No que diz respeito à metodologia que se adotou no presente estudo, assenta fundamentalmente no método do Estudo Teórico, ou seja, trata-se de um estudo da literatura científica já existe, onde procuramos não só apresentar novos avanços teóricos mediante a apresentação de nova teoria, como também permite analisar as teorias já implementadas referindo as suas próprias falhas, ou em última análise, permite apresentar as vantagens de uma nova teoria em detrimento de outras teorias já existentes. Ainda a este respeito demos, especial atenção, ao direito comparado pois permiti-nos analisar o tratamento que é feito noutros ordenamentos jurídicos à utilização do *Malware* como meio de obtenção de prova noutros ordenamentos jurídicos.

A pesquisa que efetuamos foi essencialmente, bibliográfica e documental. Em relação às fontes, que utilizamos, destacamos três grandes grupos. O primeiro reporta-se à legislação nacional, com destaque para a LC, o RJAE, o CPP e a CRP. O segundo grupo tem expressão na doutrina, isto é, um conjunto de livros, artigos, dissertações que se debruçam sobre este tema, pese embora, ainda seja escassa quando comparado com outras temáticas do DPP. No âmbito da internet, recolhemos artigos e outros documentos através do RCAAP, RESEARCHGATE, Academia Edu.

Neste contexto, a presente dissertação de mestrado encontra-se estruturada em quatro capítulos. O que pretendemos é analisar todo o regime jurídico das ações encobertas, quer em ambiente físico, quer em ambiente digital, bem como as suas figuras afins e ainda, compreender o conceito de *Malware*, não só, do ponto de vista informático, mas também no panorama do DPP, e descortinar se existe, ou não, atualmente uma aplicação prática deste conceito no nosso ordenamento jurídico enquanto meio de oculto de obtenção de prova, e questionar se eventualmente poderá vir a existir este instrumento como novo meio de obtenção de prova.

Assim sendo, o primeiro capítulo tem o intuito de analisar conceptualmente os principais temas deste estudo, o *Malware* e o AE para que exista uma melhor compreensão, por parte dos leitores, do que realmente se trata. O segundo capítulo, numa vertente jurídica, levanta desde logo problemas associados ao regime jurídico, ou falta dele, relativamente às duas realidades mencionadas, no nosso ordenamento jurídico e que fundamentam a razão de ser da elaboração da presente dissertação de mestrado.

No caso do *Malware*, a sua inexistência preocupa-nos, porque consideramos que devia constar do leque de meios ocultos de obtenção de prova no nosso ordenamento jurídico, e não faz sentido nenhum a sua ausência neste leque. Em relação às AE, sabemos que existem duas modalidades, ou seja, existe em ambiente físico cujo regime jurídico vem contemplado em legislação avulsa, nomeadamente, o RJAE e, ainda, as ações encobertas em ambiente digital igualmente regulada em legislação avulsa, de acordo com o art.º 19.º da LC, o que por sua vez, remete para o RJAE, em tudo o que for possível de aplicar. Na realidade temos efetivamente um único regime jurídico para duas realidades totalmente distintas. No entanto nós não concordamos esta previsão legal, visto que a realidade digital é muito mais ampla que a realidade física e proporciona aos criminosos uma panóplia de atividades criminosas que podem desenvolver de forma segura porque o risco de serem descobertos é nulo, ou na pior das hipóteses é mínimo, o que não se verifica em ambiente físico, porque sabemos que o risco de serem detetados é muito mais elevado e preferem não arriscar, preferem "jogar pelo seguro".

Neste sentido, aplicar o RJAE neste contexto é inofensivo, não é exequível, limita e muito a atuação do OPC no combate à cibercriminalidade. Simplesmente não faz sentido. No terceiro capítulo, o foco está na *DarkWeb,* uma "camada" da internet e que não é necessariamente um antro de criminosos que se reúnem ali para perpetrar ilícitos criminais. Todavia nos últimos largos anos, tem sido o epicentro de vários atos criminosos, o que dificulta e muito a atuação do OPC. Neste sentido importa realçar que qualquer utilizador com conhecimentos técnicos suficientes tem a capacidade de aceder à *DarkWeb*, mas isso não significa que a sua atividade seja de cariz criminoso. O utilizador apenas pretende esconder a sua atividade, mantendo o seu anonimato.

A verdade é que a maioria dos seus utilizadores utilizam este espaço para atividades criminosas. Neste contexto, consideramos necessário explicar o conceito de *DarkWeb* e outros conceitos, com o qual se pode confundir, nomeadamente, a *DeepWeb* e a *SurfaceWeb*. Posteriormente analisamos alguns programas de software que são utilizados pelos utilizadores quando navegam na *Dark* e *DeepWeb*, e que lhes garantem segurança, proteção. Finalmente vamos analisar, o conceito de criptomoedas, qual a moeda virtual mais utilizada pelos criminosos para efetuar transações neste âmbito.

Finalmente elencamos todos os meios de obtenção de prova consagrados na LC com o objetivo de analisá-los e perceber se estes meios à disposição do OPC são suficientes e eficazes, ou seja, se permitem facilmente identificar o crime e o seu agente, e se permitem ao OPC executar a atividade necessária, no caso concreto, para concluir com sucesso a investigação criminal. Por último, no quarto capítulo, analisamos se é possível, no entanto, enquadrar o *Malware* no leque dos meios de obtenção de prova e, nesse sentido, propomos uma alteração legislativa no âmbito do leque de meios ocultos de obtenção de prova que podem ser utilizados pelo OPC no contexto digital, indicando tudo o que a mesma de- verá contemplar em relação ao *Malware* neste contexto. Esta nova lei terá de ser mais densa e explicativa. Em relação ao regime jurídico das AE em ambiente digital, apesar de já ter consagração expressa no nosso ordenamento jurídico, nos termos do art.º 19.º da LC, consideramos que deveria existir um aperfeiçoamento ao seu regime jurídico, porque o atual é insuficiente para uma realidade tão ampla e complexa. Por isso consideramos que merece maior destaque face à realidade que enfrenta.

O último ponto a abordar neste estudo vai de encontro ao título e pergunta de investigação que deram início ao mesmo, onde procuramos determinar se é possível compatibilizar a utilização do *Malware* e das AE no seio da mesma investigação criminal em ambiente digital, mais concretamente na *DarkWeb.*

1. Enquadramento Concetual

Neste primeiro ponto, é importante compreender os conceitos fundamentais que suportam todo este estudo. É necessário, estabelecer definições conceptuais, quer do conceito de *Malware*, como também do agente encoberto enquanto sujeito que leva a cabo as ações encobertas e outras figuras que estão associadas aquele.

De salientar, que o *Malware* é um conceito coletivo, o que significa que, apresenta várias formas, e resulta da área da informática. Em relação ao agente encoberto encontramos várias definições na doutrina portuguesa, desenvolvidas pelos mais prestigiados penalistas do nosso ordenamento jurídico.

1.1. *Malware* e modalidades

No que diz respeito ao conceito de *Malware* encontramos várias definições em vários sites[12] da especialidade, mas a verdade é que todas elas, utilizando palavras diferentes, encontram-se no final, ou seja, podemos estabelecer uma única definição. Assim sendo, podemos definir o *Malware* como sendo um software malicioso que discretamente se instala, física ou remotamente, num sistema informático, sem o consentimento do visado, com o intuito de expor "a confidencialidade dos dados, a integridade dos dados ou a disponibilidade do sistema"[13].

[12] Por exemplo, no site da AVG, *Malware* está definido como sendo "todo e qualquer software projetado para danificar arquivos, roubar dados sigilosos, ou manter o dispositivo como refém". E carateriza-se pelo dano que pode causar num computador, ou noutro dispositivo eletrónico. Também no site do Santander, definem *Malware* como sendo um "software nocivo que interrompe ou manipula a operação normal de um dispositivo eletrónico", como por exemplo, computadores, smartphones, tablets, servidores e inclusive equipamentos domésticos, ou seja, todos os dispositivos que precisem de computação e que tenham ligação à internet. Ainda, noutros sites, como é o caso da McAfee e da Avast encontramos definições. O primeiro, começa por dizer que se trata de um "termo genérico para qualquer tipo de software malicioso (…) para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável. O segundo, diz que se trata de um "software malicioso ou código de computador projetado para infetar, danificar ou obter acesso asistemas de computador.".

[13] *In* DA SILVEIRA, MARIA ANA BARROSO DE MOURA. *Da Problemática da Investigação Criminal em Ambiente Digital – em especial, sobre a possibilidade de utilização de Malware como meio oculto de obtenção de prova.* Pp.15.

No entanto não nos podemos esquecer que este é um conceito coletivo, i.e., aplica-se a todas as modalidades de *Malware*. Logo torna-se fundamental descortinar as diferenças práticas entre as modalidades, visto que todas elas são *softwares* maliciosos, mas apresentam características únicas para atingir os mais variados objetivos. Neste âmbito, podemos encontrar, o *cavalo de troia*; o *spyware*; o *keyloggers*; os *rootkits*; as *logic bombs*; o *vírus* e worms, e finalmente o *ransomware*.

O cavalo de troia, tem como objetivo aceder remotamente a um sistema informático, de forma oculta sem que o seu utilizador tenha conhecimento de toda a situação atempadamente. Normalmente ludibria o utilizador disfarçando-se num ficheiro, num *website* aparentemente inofensivo, numa mensagem do correio eletrónico, no qual encontramos um anexo, ou até mesmo quando abrimos uma página da internet e a mesma se encontra infetada, com o único objetivo de esconder a sua verdadeira finalidade. Esta modalidade de *Malware* tem a capacidade de se multiplicar infetando múltiplos ficheiros. no entanto para ser executado precisa de outros meios[14], porque sozinho não é possível infetar um dispositivo eletrónico. Através deste *Malware* é possível ao agente eliminar, modificar ou reproduzir todos os ficheiros do computador[15] visado, como também pode obter credenciais de acesso e outras informações confidenciais.

Consegue desativar os programas de antivírus que estejam a proteger o computador e principalmente podem monitorizar toda a atividade que é levada a cabo no computador que se encontra infetado, ou seja, ao abrirem *backdoors*[16], podem assumir o controlo total sobre o computador visado o que permite, além do que foi mencionado, enviar documentos e informação diretamente para o agente que o criou.

[14] Como por exemplo, drive-by-downloads; exploração de vulnerabilidade, download através de um outro *Malware* ou até mesmo mediante técnicas de engenharia social.
[15] Ou qualquer outro dispositivo eletrónico.
[16] Pode ser definido como sendo uma "porta aberta" não autorizada que permite ao seu utilizador entrar num sistema que não lhe pertence, sem acionar os sistemas de proteção ou descobertos pelo utilizador atempadamente. Normalmente, só quem tem acesso a estes são os fabricantes do software em questão. Os *backdoors,* podem ser utilizados para efeitos legítimos, por exemplo, nas empresas quando é preciso resolver algum problema ou fazer a manutenção do sistema, o fabricante a pedido da empresa pode entrar remotamente no sistema através do *backdoor* sem ter de se deslocar à sede da empresa. O problema dos *backdoors* é que podem ser utlizados como meio de propagação do *Malware* infetando o sistema em questão, permitindo ao *hacker*

O *Spyware*, é fundamentalmente um programa informático que absorve toda a informação sobre uma determinada pessoa ou organização sem o seu devido consentimento ou conhecimento, ou seja, tal com o seu nome indica, este *Malware* permite ao seu agente espiar o dispositivo eletrónico que pretende com o intuito de obter todos os dados pessoais que possa, nomeadamente, nomes, moradas, emails, *passwords*, dados de cartões de crédito e dados bancários, ou até mesmo a o histórico de todos os *websites* visitados naquele computador e, em algumas situações, pode enviar essa informação para terceiros. Toda a recolha de informações financeiras através deste *Malware* concede ao seu utilizador o poder de aceder à conta bancária da vítima, deixando-a sem qualquer dinheiro, podendo assim financiar outras atividades ilícitas. O *Spyware* pode se encontrar escondido num email ou num anexo de uma mensagem que correio eletrónico, como também podem estar escondidos em anúncios indesejados que surgem quando se visita páginas da internet, ou janelas *pop-up.* Outro meio de o *Spyware* recolher a informação que precisa é através da utilização em conjunto de uma outra modalidade de *Malware*, os *Keyloggers*. Na esmagadora maioria, os *Spywares*, tem a capacidade de se atualizar automaticamente, fazendo *download* de novas atualizações, o que permite aplicar novas funcionalidades e evitar que seja detetado pelos programas de antivírus. Esta modalidade de *Malware* está muitas vezes interligada a uma outra modalidade que irá ser desenvolvida em seguida, os *Keyloggers*.

Os *Keyloggers* são muitas vezes utilizados em conjunto com o *Spyware*, mas também podem se encontrar associado a outro *Malware*, com a finalidade de espionar as suas vítimas, permitindo ao seu utilizador capturar tudo o que é escrito no teclado, desde nomes de usuário a *passwords* ou até mesmo n.ºs de conta bancária, mensagem privada, observar as conversas tidas com outras pessoas por email ou mensagens, o histórico de navegação e pesquisa, controlar remotamente o dispositivo, ou inclusive fazer login ou log out, do dispositivo remotamente, sem o consentimento do utilizador. Além do mais tudo o que é escrito no teclado de um dispositivo eletrónico fica gravado com o intuito de obter informações pessoais sobre os seus alvos.

alterar, eliminar todo o tipo de dados que estejam no sistema e até mesmo instalar outras modalidades de *Malware*, atendendo ao seu objetivo final.

Esta modalidade de *Malware* pode ser utilizada de dois modos, quer através de *hardware*, quer através de *software*. A primeira, raramente é utilizada, visto que implica um acesso ao local físico em que se encontra o dispositivo e normalmente é utilizado sob a forma de uma *pen drive*, ao passo que a segunda, é a mais frequente pois não é necessário um acesso físico ao dispositivo que se pretende atingir. Através do *software* este *Malware* funciona como qualquer outro, infiltra-se no dispositivo através de anexos que aparentemente são inofensivos, e também podem esconder-se noutro *Malware*, como por exemplo, o cavalo de troia. Tudo o que é digitado e recolhido por este *Malware* é enviado regularmente para o seu utilizador, quer por email, ou até mesmo serem transferidos para um site. Quando os *keyloggers* são utilizados através de *uma pen drive* e instalados fisicamente, toda a informação que foi recolhida fica armazenada no dispositivo até ao momento em que o *hacker* recupere o dispositivo utilizado para introduzir o *Malware* no computador.

Os *rootkits,* podem ser definidos como sendo um conjunto de programas maliciosos que tem em vista alterar o sistema operacional do dispositivo eletrónico que pretendem atacar, com o objetivo de ocultar a invasão e a presença do invasor e de outro *Malware* que possa ter sido instalado em conjunto com os *rootkits,* do usuário daquele dispositivo. A sua única função é ludibriar o usuário ou o administrador do sistema visado fazendo crer que está tudo a funcionar normalmente quando na verdade esse sistema foi invadido por outrem, e o *hacker* já tomou controlo desse sistema podendo utilizá-lo para qualquer atividade ilícita que pretenda sem que o utilizador ou o administrador tenham conhecimento do que está a acontecer naquele momento. Os *rootkits* em conjunto com outro *Malware* podem atacar não só dispositivos eletrónicos como também sistemas informáticos recolhendo dados pessoais do usuário ou até mesmo utilizar um determinado sistema informático como ponte para outros sistemas informáticos o que dificulta o seu rastreamento.

Os *Logic Bomb,* não são propriamente *Malware*, mas são constantemente associados a várias modalidades de *Malware*. São fundamentalmente ataques sofisticados, mas que produzem efeitos devastadores. Este código malicioso é introduzido secretamente nos dispositivos eletrónicos, nos sistemas operacionais ou até mesmo em softwares. Estas "bombas" ficam adormecidas até à verificação de uma determinada condição, ou evento, v.g., data e hora especifica ou download de algum anexo infetado com estes ataques. Esta condição normalmente corresponde a um determinado facto e, a partir do momento em que se verifica faz automaticamente despoletar o ataque que até então estava adormecido corrompendo todo um sistema informático bem como os seus dados, podendo bloquear o acesso a documentos por parte do próprio administrador tornando-se impossível restaurar o seu acesso.

Os *vírus* e *worms*, vão ser analisados em conjunto porque os seus efeitos práticos são fundamentalmente os mesmos, distinguindo-se exclusivamente pela forma como são usados. O que tem em comum é o facto de serem modalidades de *Malware* e que se alastram rapidamente. O *vírus*, em particular, propaga-se de dispositivo em dispositivo eletrónico, mas primeiro precisam de um hospedeiro onde se esconder, quer seja num anexo ou num documento. O *vírus* associa-se a outros programas, e assim consegue replicar-se noutros dispositivos, e a partir desse momento pode anexar-se noutros arquivos e documentos guardados nesse mesmo dispositivo e se alguma vez forem enviados, o dispositivo que os receber ficará igualmente infetado com o *vírus* e assim sucessivamente. Fundamentalmente o *vírus* informático funciona na mesma lógica que os *vírus* que afetam os indivíduos. Quando as pessoas ficam infetadas com um *vírus* depois de terem estado em contacto com uma outra pessoa já contaminada. Em sentido inverso, os *worms* são programas autónomos que se multiplicam e espalham automaticamente, subsistem por si mesmo, não necessitam de nenhum hospedeiro, e a sua ativação não depende do usuário. São mais perigosos do que o vírus pois tem a capacidade de se reproduzirem em todos os contactos do email do usuário infetado, e assim sucessivamente.

Finalmente o *Ransomware* pode ser definido como sendo uma modalidade especifica de *Malware* que impede o acesso do usuário aos seus próprios dados criptografando-os e exigindo um resgate ao usuário para que este volte a ter, novamente, acesso aos dados que outrora lhe foram negados pelo *hacker* e, caso não efetue esse pagamento ameaçam destruir todos os documentos que se encontram bloqueados[17]. Pelo facto de exigirem um resgate às suas vítimas, quer sejam pequenas ou grandes empresas, quer sejam pessoas comuns, o *Ransomware* torna-se muito lucrativo para os seus utilizadores e, por isso é utilizado especialmente em crimes de extorsão digital, mas também lhes permite correr menos riscos. Porque vendem a informação que tem em seu poder a terceiros, não necessitam um encontro pessoal para fazer essa transação. Podemos afirmar que esta palavra deriva da fusão entre duas outras palavras: *ransom*, que significa resgate, e *Malware*, que significa programa malicioso, ou seja, é um *Malware* que tem como objetivo principal exigir dinheiro às suas vítimas e para atingir esse fim, consegue bloquear e reter todos os dados pessoais e financeiros num determinado dispositivo eletrónico, até o resgate ser efetuado. Este resgate normalmente é efetuado por via das criptomoedas.

O *Ransomware* inicialmente só causava problemas à plataforma *Windows*, mas a verdade, é que com o passar dos anos, a sua sistemática evolução permitiu aos *hackers* atacarem outras plataformas, v.g., *Apple*, *Android* e *Linux*. Ainda sobre o *Ransomware*, importa referir que se subdivide em três categorias[18]: o *scareware, o locker-ransomware* e finalmente, o *crypto-ransomware*. A utilização do primeiro, permite ao seu agente fazer-se passar uma autoridade que visa alertar a sua vítima para efetuar determinado pagamento, caso contrário sofrerá as legais consequências. Nesta situação, não existe qualquer perigo real para as vítimas, é apenas uma forma de os hackers assustarem as suas vítimas levando-as a efetuar o referido pagamento. Outras vezes, o *scareware* pode adotar a forma de *leakware*, ou seja, cria na vítima a ideia de que se não pagar, toda a sua família e amigos ficam a saber de algo que não deviam.

[17] *In* SEGUIN, PATRICK e LATTO, NICA. *Guia Básico sobre Ransomware.* Artigo publicado a 24de setembro de 2021.
[18] *In* ESET. *Guia de Ransomware.*
Disponível em: 2021-ESET-guia-ransomware-PT.pdf

A utilização do segundo, permite bloquear o sistema que se pretende atingir, no entanto, este é o menos perigoso, visto que a própria vítima, por si, pode resolver o problema desde que reinicie de modo seguro o sistema. O mais perigoso é, efetivamente, o último, o *crypto-ransomware*, que criptografa todos os documentos e arquivos da vítima, impedindo que a mesma tenha acesso a eles, a menos claro, que efetue o resgate. Posto isto podemos referir, que o Ransomware é extremamente eficaz explorando a fraqueza humana mediante o uso de táticas de engenharia social[19], isto é, uma estratégia psicológica que leva a vítima a atuar da forma como o atacante pretende, com o único objetivo de obter acesso não autorizado a toda a informação constante num determinado sistema ou dispositivo eletrónico. Esta modalidade de *Malware*, pode se esconder em aplicações, propagandas aparentemente legitimas, nas redes sociais ou nos vários anúncios removíveis que surgem quando visitamos sites na internet.

1.2. Agente Encoberto e figuras afins

Com exceção do agente encoberto, sempre que nos referimos às figuras afins reportamo-nos a três conceitos distintos, nomeadamente: o agente infiltrado, o agente provocador e, ainda, os terceiros infiltrados também conhecidos por homens de confiança.

No que diz respeito a estas distinções, importa referir que a doutrina e a jurisprudência não concordam quanto à autonomização do conceito de agente infiltrado, isto é, enquanto a doutrina faz a distinção entre agente encoberto e agente infiltrado, pese embora sejam realidades muito semelhantes, a jurisprudência não opta por essa distinção utilizando ambos os conceitos indiferenciadamente para referir a mesma realidade, ou seja, considera que a distinção que se faz entre agente encoberto e agente infiltrado não tem qualquer relevância prática visto que a lei n.º 101/2001 aplica-se a ambas as figuras sem fazer distinção entre as mesmas[20].

[19] *In* KOVACS, LEANDRO. *O que é engenharia social?*. Artigo publicado em 2021 e atualizadoem 2023.
[20] *In* RAMALHO, DAVID SILVA. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* p. 283. Coimbra. Almedina. 2017, reimpressão de 2019.

O principal fator de diferenciação, analisado em seguida, entre estas duas realidades assenta no facto de o agente encoberto apenas observar a situação e o desenrolar dos acontecimentos, sem intervir ou estabelecer uma relação de confiança[21]. Ainda, sobre o agente encoberto e as figuras afins é importante destacar que se aplicam quer às ações encobertas em ambiente físico quer às ações encobertas em ambiente digital, algo que as modalidades de ações encobertas têm em comum, no entanto, existem algumas diferenças entre elas que serão analisadas no seu devido momento.

Como já enunciado anteriormente, além da definição de AE[22], existem outras designações no âmbito desta matéria, sobejamente conhecidas como figuras afins, que importam destacar realçando, as suas principais diferenças comparativamente ao agente encoberto, consagrado legalmente no RJAE. Para efeitos do presente estudo é importante explicar que existe esta distinção, e em que é que consiste. Assim sendo, iremos adotar, o ponto de vista da doutrina pelo que será feita a distinção entre estes conceitos, principalmente, entre o agente encoberto e o agente infiltrado, pese embora, alguns autores considerarem inútil tal diferenciação. No entanto, consideramos que esta distinção não faz sentido e que estamos perante duas realidades iguais. Logo podemos utilizar indiferenciadamente, estes dois conceitos para referir a mesma realidade.

Segundo DAVID SILVA RAMALHO[23] a distinção que se pretende fazer entre agente encoberto e agente infiltrado acarreta duas desvantagens, por um lado, é inútil e, por outro lado, pode causar confusão visto que se está a distinguir duas realidades que na verdade são bastante verossímeis. Em relação ao agente encoberto, podemos caracterizá-lo pela ocultação, ativa ou passiva, da verdadeira identidade do agente associada à sua interação com terceiros mediante a utilização de uma identidade fictícia, com o intuito de conquistar a confiança destes facilitando a recolha de prova.

[21]Cf. RAMOS, ARMANDO DIAS. *O Agente Encoberto Digital. Meios Especiais e Técnicos de Investigação Criminal.* P.55. Coimbra. Almedina. 2018.
[22] Trata-se de um conceito jurídico inserido no âmbito do DP, funcionando como um meio ocultode obtenção de prova para a descoberta da verdade material.
[23] *In* RAMALHO, DAVID SILVA. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* p. 289 Coimbra. Almedina. 2017, reimpressão de 2019.

O autor MANUEL ALVES MEIRELES[24], é um dos autores que defende a distinção entre estas duas figuras. Segundo este autor, o agente encoberto é um agente da polícia, ou alguém às ordens deste, que visita locais que normalmente são frequentados por criminosos e, sem nunca revelar a sua identidade, limita-se a recolher todos os indícios que possam existir, sem nunca interferir no normal rumo dos acontecimentos. É importante referir que em toda a sua ação, o agente encoberto, não provoca o crime, nem conquista a confiança de ninguém. É um mero observador do crime.

Em sentido contrário, o mesmo autor[25], vem dizer que o agente infiltrado é alguém que não só acompanha toda a atividade criminosa como também pratica atos sempre que seja necessário, sob pena de ser descoberta a sua identidade. Assim sendo, para este autor, o agente infiltrado é a mesma realidade a que lei atribui o nome de agente encoberto, por força da nomenclatura dada ao diploma, ações encobertas.

Ainda sobre o conceito de AE, é necessário referir que comporta três elementos fundamentais[26] que merecem o seu destaque individual[27], e que ajudaram a compreender melhor o conceito de AE já enunciado, e que são bem demonstrativos da sua perigosidade, por isso se trata de um meio oculto de obtenção de prova, porque não pode ser utilizado constantemente, apenas em casos muito excecionais e depois de verificados todos os seus pressupostos de utilização, a começar pelo catálogo taxativo de crimes. O primeiro elemento reporta-se à identidade oculta do agente no ambiente em que se pretende integrar, ou seja, não só se limita a esconder a sua identidade como também, se for necessário, mente sobre a mesma caso lhe sejam colocadas questões. No segundo elemento, já estamos na fase da infiltração, quando o agente procura efetivamente entrar num ambiente de criminalidade, quer seja de forma passiva ou ativa.

[24] Cf. GUEDES, ANA RITA ALMEIDA. *O Agente Encoberto Digital enquanto Método Oculto de Obtenção de Prova.* p. 11. Dissertação no âmbito do 2º ciclo de Estudos em Ciências Jurídico-Forenses. Universidade de Coimbra. Coimbra, outubro de 2021.
[25] *Idem.*
[26] *Ibidem.* p. 292 ss.
[27] Os referidos elementos serão analisados quer do ponto vista das AE em ambiente físico, quer do ponto de vista das AE em ambiente digital, visto que se aplicam a ambas as modalidades de AE.

Se for passivamente, o agente limita-se observar os acontecimentos e recolher as informações que considera cruciais para o sucesso da investigação. Em sentido oposto a integração neste ambiente será ativa se o agente procurar estabelecer contacto com os suspeitos criando uma relação de confiança com os mesmos. O último elemento, reporta-se à necessidade da ação encoberta, ou seja, depois de ativamente ocultar a sua identidade e de se integrar num ambiente de criminalidade resta ao agente encoberto recolher a prova. As recolhas de prova nas AE pretendem não só demonstrar a intenção, ou a efetivação, do cometimento de ilícitos criminais responsabilizando criminalmente o suspeito ou então permitirá prevenir outros crimes que aqueles suspeitos já estavam a preparar cometer.

Agora do ponto de vista das AE em ambiente digital, o primeiro elemento não acrescenta nenhuma novidade visto que a ação encoberta pode ser totalmente desenvolvida através de um dispositivo eletrónico sem qualquer contacto pessoal entre o agente encoberto e os suspeitos. A interação entre agente encoberto e os suspeitos, em ambiente digital, é incomparável com a interação que existe entre os mesmos intervenientes, num ambiente físico. Muitas vezes os utilizadores não sabem quem são as pessoas com quem interagem, nomeadamente, o aspeto físico e, muito menos, o local onde se encontram naquele momento, ou o seu país de origem.

Além do mais, é um meio onde todos os seus utilizadores, criminosos ou não, utilizam, na maioria nomes fictícios[28]. Em relação à infiltração por parte do agente encoberto, ela verifica-se com o simples registo de acesso a um fórum, *website*, entre outros. Em relação à recolha de prova do cometimento do ilícito criminal ou da iminência do seu cometimento a principal dificuldade é saber a que individuo imputar. Com exceção, desta questão, a recolha de prova mostra-se mais fácil em ambiente digital do que em ambiente físico visto que naquele existe muita informação que pode servir como prova e sem necessidade de manter contacto ou iniciar uma interação com o suspeito.

[28] O u*sername* ou *nickname*, são muitas vezes, utilizados pelos utilizadores da internet independentemente da atividade que desenvolvem na internet. Apenas utilizam os seus nomes verdadeiros quando é estritamente exigido e não existe outra forma de aceder.

Em ambiente digital, agente encoberto para recolher prova, apenas necessita de um nome fictício e depois integrar, v.g., um grupo, fóruns ou *websites*, blogs, pode simplesmente ficar a assistir, sem intervir, omitindo a sua identidade, mas sempre pronto a recolher todas as informações que podem ser utilizadas como prova.

O principal fator diferenciador entre o agente encoberto e o agente infiltrado, dando já a tónica para a definição deste último, reside no facto de o agente encoberto apenas estar presente no desenrolar dos acontecimentos sem interferir, de modo algum, ou conquistar a confiança de terceiros que estejam envolvidos, i.e., funciona como um simples espetador que observa o decorrer das ações recolhendo toda a informação que necessita. Podemos comparar o agente encoberto ao que normalmente se refere de agente à paisana. Nas palavras de VALENTE[29], a lei n.º 101/2001, bem como todos os diplomas legais que utilizam a expressão "ação encoberta" estão verdadeiramente a referir-se ao agente infiltrado e ao desenvolvimento das suas atividades. Por isso ONETO**[30]**, vem afirmar que o agente encoberto é uma modalidade do agente infiltrado.

Em sentido contrário, o agente infiltrado é aquele OPC ou terceiro, atuando sob a direção daquele que não se limita a ocultar a sua identidade como ainda consegue estabelecer uma relação de confiança com os suspeitos, intrometendo-se no meio onde ocorrem atividades criminosas, sem qualquer interferência no resultado que se pretende, nomeadamente, com a prática do ilícito criminal, informando as autoridades competentes da prática destas atividades. O seu principal objetivo é a recolha de prova sem provocar a prática do ilícito criminal para o atingir.

[29] Cf. MANN, DIANA CALAZANS. *Infiltração Digital: A validade como meio de prova e os limites éticos do Estado-Investigador.* p.9. Dissertação do VII Mestrado não integrado em Ciências Policias no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI), especialização em Criminologia e Investigação Criminal.

[30] *In* MONTEIRO, ERICK WALLACE CARNEIRO CALAÇA DIAS. *Ações Encobertas no Mundo Virtual: a problemática da tutela da privacidade como barreira à obtenção de provas nas redes sociais.* P.23. Dissertação de mestrado científico em Ciências Jurídico-Criminais. Lisboa, 2018.

No âmbito desta figura, é importante realçar que existem vários graus de infiltração desde a ausência de contacto com os agentes do crime até à sua infiltração em posições cimeiras de uma organização criminosa. Em relação ao agente infiltrado, VALENTE[31] afirma que este é consagrado, pela doutrina, como um meio oculto de obtenção de prova, consubstanciando uma técnica de investigação moralmente duvidosa pois o suspeito irá, involuntariamente, produzir a prova necessária para que ele próprio seja condenado pela prática do ilícito criminal, o que irá afetar as garantias processuais do arguido.

A outra figura que merece destaque é o agente provocador, o qual é absolutamente proibido por lei como veremos oportunamente. Este agente é exatamente o oposto do que vimos em relação ao agente encoberto e ao agente infiltrado. O agente provocador é um OPC, ou terceiro que atua sob a direção daquele, e que motiva outro sujeito ao cometimento de um ilícito criminal, que em momento algum se verificaria se não fosse pela conduta do OPC ou de terceiro, com o objetivo de recolher prova da prática do ilícito mais rapidamente. Ou seja, o agente nunca teria cometido o crime se não fosse pela intervenção motivada do OPC em recolher a prova que precisa[32]. O agente provocador ao integrar-se num meio criminoso, demonstra ter um papel preponderante intervindo na génese do cometimento do crime, não se limitando à mera observação do ato previamente decidido pelo suspeito.

A principal distinção entre esta figura e as anteriormente enunciadas, reside fundamentalmente no facto de o agente provocador instigar uma intenção, inexistente até aquele momento, de levar a cabo um ilícito criminal. Algo que contraria tudo o que sabemos sobre a finalidade do processo penal[33], visto que o OPC estaria a criar um crime a partir do qual iria recolher prova para condenar alguém que estaria inocente desde o princípio, mas que foi levado a cometer o crime por outrem.

[31] Cf. MANN, DIANA CALAZANS. *Infiltração Digital: A validade como meio de prova e os limites éticos do Estado-Investigador.* p.6.Dissertação do VII Mestrado não integrado em Ciências Policias no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI), especialização em Criminologia e Investigação Criminal.

[32] Por exemplo, se estiver a ser pressionado por um superior hierárquico, que aguarda novidades. Ou então em situações que quer mostrar as suas competências. Ou seja, em situações de elevado stress.

[33] Entendida como a realização da justiça através da perseguição criminal dos culpados.

Segundo GERMANO MARQUES DA SILVA[34], a existência de provocação não expõe o crime e o criminoso, mas sim cria-os, e como tal, essa situação é contrária ao objetivo final da investigação criminal. Como já elencado, a atuação do agente provocador é proibida nos termos da lei por clara violação do princípio democrático e da lealdade[35] e o direito a um processo justo e equitativo[36]. Aliás, trata-se de um meio enganoso que viola a integridade moral do visado pelo que toda e qualquer prova obtida com recurso ao agente provocador deverá ser considerada nula[37]. Além do mais consubstancia um meio enganoso não legitimado e, como tal, ofensivo da integridade moral do visado, pelo que a prova obtida através dele será nula, por força do disposto no n.º 8 do art.º 32.º da CRP e na al. a) do n.º 2 do art.º 126.º do CPP.

Finalmente, a última figura que nos falta abordar, são os terceiros infiltrados, também designados por homens de confiança. É frequentemente utilizada nos EUA[38], como sendo informadores, aliás nós conhecemo-los como sendo os *undercover agents*. Esta figura surgiu porque em determinadas situações é muito complicado, até mesmo inviável, infiltrar um OPC num ambiente criminoso, v.g., integrando num grupo de criminosos, ou até mesmo uma interação com o suspeito com a finalidade de recolher provas ou informações relevantes. Por isso, como alternativa o OPC tende a recorrer a um cidadão[39].

[34] *In* ANDRADE, MANUEL DA COSTA. *"Bruscamente no verão passado", a reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente.* Coimbra Editora, 2009.
[35] Cf. Art.º 1.º, 2.º e al. b) do 9.º da CRP.
[36] Com base no Art.º 20.º CRP.
[37] Por força do disposto no n.º 8 do art.º 32.º da CRP e da al. a) do n.º 2 do art.º 126.º do CPP. [38] Atendendo ao facto de que nos EUA existem múltiplas agências governamentais legitimadaspara se socorrerem deste meio, nomeadamente: DEA, FBI, CIA, IRS, U.S MARSHALSSERVICE, NYCPD, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, BUREAU OFALCOHOL TOBACCO FIREARMS AND EXPLOSIVES.
[39] Denominado de homem de confiança em sentido restrito. Sem qualquer conexão direta com oOPC.

No entanto este cidadão, não é um mero civil, isto é, trata-se de alguém que pelos contactos, conhecimentos específicos sobre o crime que se está a investigar ou, inclusive, que já tenha estado associado a esse mesmo crime, terá uma maior facilidade em se integrar num determinado grupo de criminosos estabelecendo relações de confiança com os mesmos e assim recolher toda a informação que é pretendida e que de outro modo seria impossível, ou que dificilmente, o OPC teria acesso. Para ONETO[40], é fundamental referir algumas considerações que devem ser feitas no âmbito desta figura. Desde logo, o seu pagamento, ou seja, estes cidadãos não sendo OPC, ao envolverem-se numa investigação tão perigosa esperam ser recompensados pecuniariamente o que não tem problema nenhum, a não ser o facto de estes normalmente receberem valores mais elevados quando comparado com os pagamentos feitos ao OPC que desempenham estas funções, do ponto de vista do agente encoberto.

A outra questão que suscita dúvidas e que ONETO refere, é a falta de transparência no recrutamento destes terceiros infiltrados. Por norma desconhece-se o critério utilizado, podendo se tratar quer de um individuo com informações relativamente ao modus operandi dos criminosos sob investigação ou então o facto de ser alguém que já está inserido no ambiente criminoso e, portanto, escusa estabelecer relação de confiança, como normalmente sucede com o agente infiltrado, visto que essa relação já está estabelecida.

O que leva estes terceiros a envolverem-se numa investigação tão perigosa, acarretando riscos para a sua própria vida como esta, assenta fundamentalmente sempre nos mesmos motivos, independentemente do terceiro envolvido. Normalmente o terceiro decide envolver-se: por uma compensação pecuniária associada ao seu envolvimento, pelo medo de serem punidos se forem arrependidos[41]; pelo desejo de vingança ou o receio de represálias quando sejam ex-membros de um grupo; pela vontade em verem a sua pena ser diminuída.

[40] *In* MANN, DIANA CALAZANS. *Infiltração Digital: A validade como meio de prova e os limites éticos do Estado-Investigador.* p.7. Dissertação do VII Mestrado não integrado em Ciências Policias no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI), especialização em Criminologia e Investigação Criminal.

[41] Visto que se trata de pessoas que anteriormente estavam envolvidas num determinado grupo de criminosos, mas que durante aquele período se arrependeram e decidiram ajudar as

No fundo, todos os motivos são válidos, desde que sejam legalmente admissíveis no Estado em questão, ou seja, a sua motivação para ajudar na investigação e o seu interesse pessoal na mesma tem de ser levado a consideração no âmbito da valoração probatória. Ainda sobre o terceiro infiltrado, no âmbito da investigação criminal em ambiente digital, a sua utilidade é de especial importância não só quando se trata de um terceiro que esta presente no meio criminoso que se pretende investigar, mas também quando o terceiro tenha conhecimentos técnicos que lhe permitem integrar em ambientes considerados inacessíveis aos agentes da autoridade.

Todavia, no âmbito desta figura, existe uma questão muitas vezes colocada que é de saber se o individuo que atua como terceiro infiltrado pode ser alguém que já cometeu crimes, antes de se dar início à ação encoberta, na área que se pretende investigar. A resposta parece afirmativa visto que no ordenamento jurídico português, nomeadamente, em legislação processual penal, não existe qualquer impedimento que exclua o suspeito ou o arguido de se tornarem terceiros infiltrados, pese embora, o cometimento de crimes.

No entanto, é preciso referir que esta situação não pode ser utilizada constantemente, isto é, só pode ser utilizada como uma alternativa, apenas em situações de extrema necessidade não existindo nenhuma outra possibilidade de levar a cabo a ação encoberta. Em relação aos terceiros infiltrados é necessário referir que nem tudo é positivo, ou seja, também acarreta algumas desvantagens que são por demais evidentes e que precisam ser reveladas, principalmente nas ações encobertas em ambiente físico. Desde logo o facto, de as declarações prestadas por estes em sede de julgamento vão ser consideradas no âmbito do regime jurídico aplicado ao coarguido[42] e nunca no âmbito do regime aplicável às testemunhas[43].

autoridades a desmantelarem esse mesmo grupo, ou simplesmente, a prevenir o cometimentode um crime.

[42] Cf. n.º 3 do art.º 345.º CPP.

[43] Segundo a al. a) do n.º 1 do art.º 133.º CPP.

Outro aspeto negativo é falta de interesse deste sujeito em integrar-se na investigação, a não ser, que tenha algum interesse nisso. Se analisarmos esta figura no âmbito das AE em ambiente digital veremos que estas desvantagens são atenuadas, visto que a atuação do terceiro infiltrado é constantemente controlada pela autoridade judiciária, inclusive a sua recolha de prova, concedendo-lhe um estatuto autónomo que não lhe seria atribuído se participasse numa AE em ambiente físico. Neste sentido, o terceiro infiltrado não precisa ter uma participação ativa na investigação, ou seja, no âmbito das AE em ambiente digital dado o seu complexo contexto bastará ao terceiro infiltrado disponibilizar ao agente encoberto as suas credenciais de acesso aos fóruns, *websites*, entre outros, para que este possa recolher a prova. Por outras palavras, o terceiro infiltrado não necessita executar quaisquer atos, propriamente ditos, bastará fornecer toda e qualquer informação que o agente encoberto precisa para ludibriar os suspeitos utilizando a identidade do terceiro infiltrado visto que em ambiente digital o contacto físico e visual não é necessário para levar a cabo a AE. Quando nos referimos a esta troca de informação entre o terceiro infiltrado e o agente encoberto não nos reportamos exclusivamente às credenciais de acesso como também à troca de conhecimentos técnicos[44] que permitiram ao agente encoberto ter sucesso na sua investigação.

2. Enquadramento Legal: LC e RJAE

O que pretendemos é precisamente por um lado, averiguar se existe atualmente no nosso ordenamento jurídico alguma disposição legal, quer no âmbito do CPP, quer no âmbito da LC, que permita a aplicabilidade do *Malware* como meio oculto de obtenção de prova e verificarmos também o que acontece noutros ordena- mentos jurídicos.

[44] Atendendo à finalidade da AE, por vezes, os agentes encobertos não tem conhecimentos técnicos e práticos e é importante que o terceiro infiltrado, normalmente alguém associado a um determinado crime ou grupo criminoso, passe todos os conhecimentos que têm ao agente encoberto para que este possa desempenhar o seu papel na perfeição sem comprometer o seu disfarce.

Relativamente à LC, importa referir que foi publicada no nosso ordenamento após a assinatura de Portugal na Convenção da Cibercriminalidade[45]. Esta Convenção permitiu bloquear e, consequentemente, criminalizar a prática de atos contrários à "confidencialidade, integridade e disponibilidade dos sistemas (…) redes e dados informáticos", bem como a utilização fraudulenta desses sistemas, redes e dados"[46], e ainda criar competências que sejam suficientes para que de uma forma eficaz se possa combater estes ilícitos tornando mais fácil a investigação criminal e, consequente, ação penal que incida sobre estes ilícitos, quer no panorama nacional, quer no panorama internacional com a criação de normas no âmbito da cooperação internacional. Tem igualmente atenção, ao equilíbrio que deve existir entre a aplicação da nova lei e o respeito pelos DLG[47].

O principal destaque que será feito à referida Convenção tem por base o art.º 20.º e 21.º do título V da mesma, nos quais se prevê, respetivamente, não só, a possibilidade de recolha, em tempo real, de dados de tráfego e a interceção, como também a recolha, em tempo real, dos dados de conteúdo que reportem às comunicações. Como veremos, o legislador quando elaborou a LC, não teve em consideração estes dois preceitos legais como deveria ter feito, e essa é uma das críticas que fazemos a este diploma legal, o facto de não contemplar a recolha de prova em tempo real.

Por outro lado, analisaremos o regime jurídico aplicável às AE, quer em ambiente digital quer em ambiente físico e, como veremos, o regime jurídico, consagrado no ordenamento jurídico português, é idêntico quer nas AE em ambiente físico como também nas AE que se verificam em ambiente digital.

---

[45] Ou Convenção de Budapeste, de 2001. Esta convenção tem como objetivo proteger a sociedade contra o cibercrime através do desenvolvimento de uma política criminal comum, assente na cooperação internacional e na adoção de legislação, por parte dos Estados, conforme aquela realidade, permitindo um combate justo por parte das autoridades responsáveis. Esta Convenção permite completar outras Convenções elencadas no preambulo, v.g., a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, presente Convenção com o objetivo de melhorar a eficácia das investigações e. respetivas, ações penais que incidam sobre os sistemas e dados informáticos. *In* Convenção do Cibercrime. p.13.
Disponível em: Convenção sobre o Cibercrime | Portal do Ministério Público - Portugal (ministeriopublico.pt).

[46] Preambulo Convenção de Budapeste. P.13. *in.* 0635406378.pdf (dre.pt).

[47] Consagrados na Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa. *Idem.*

Em seguida, demonstraremos as diferenças evidentes que existem entre estas duas modalidades de AE com o objetivo de comprovar que o regime jurídico aplicado às AE em ambiente físico torna-se insuficiente quando aplicado às AE em ambiente digital em virtude das infinitas possibilidades de executar um ilícito criminal neste novo mundo que é o cibercrime, e que está em constante evolução. É por demais evidente a escassez de base legal especifica dedicada às ações encobertas em ambiente digital, algo que acontece, não só no nosso ordenamento jurídico como também noutros Estados[48].

2.1. Malware

No que diz respeito ao enquadramento legal do *Malware*, importa referir que atualmente não existe qualquer legislação no nosso ordenamento jurídico, em especial na LC, que consagre expressamente, ou tacitamente, a utilização do *Malware* como meio oculto de obtenção de prova. É neste contexto que surge a nossa principal crítica à elaboração deste diploma. Como supramencionado, este diploma existe no nosso ordenamento jurídico, e noutros, embora com distinta nomenclatura, por força da Convenção do Cibercrime assinada por Portugal em Budapeste, no ano de 2001. Também já vimos que esta Convenção estabelece a criação de meios de obtenção de prova que permitem a recolha de prova em tempo real[49].

E por força desta Convenção, desde 2001, os Estados que a assinaram[50] podem nos seus ordenamentos jurídicos, implementar novas medidas legislativas que prevejam alguns, ou todos, os meios de obtenção de prova que se encontram consagrados na Convenção do Cibercrime. A título de exemplo, e reportando exclusivamente ao que se discute, o legislador alemão contemplou no ordenamento jurídico,

[48] *In* RAMALHO, DAVID SILVA. *métodos ocultos de investigação criminal em ambiente digital*. p.283. 2017, Almedina.
[49] Conforme arts.º 20.º e 21.º, titulo V, da referida Convenção. pp. 18-19. *In* 0635406378.pdf (dre.pt).
[50] Cf. n.º 1 do art.º 36.º da mesma. p.23. *idem*. Segundo o qual, quer sejam Estados Membros do Conselho da Europa, como Portugal, quer Estados que não sejam membros do Conselho da Europa tenham contribuído para a elaboração da presente Convenção.

a utilização do *Malware* como meio de obtenção de prova[51]. Em sentido contrário o legislador português não adotou esse entendimento, e decidiu não incluir este instrumento no leque dos meios ocultos de obtenção de prova, quando a Convenção claramente permite essa possibilidade ao utilizar a expressão, "em tempo real", quer no art.º 20.º, quer no art.º 21.º.

Se analisarmos todos os meios de obtenção de prova que se encontram regulados na LC, desde o art.º 11.º ao 19.º, em nenhum deles encontramos a referência a esta expressão e, como já vimos, no capítulo anterior, o *Malware* permite o rastreamento em tempo real de toda a atividade desenvolvida pelo individuo no dispositivo eletrónico, ou no sistema informático, inclusive aceder remotamente à *webcam* e ao microfone. Neste sentido, podemos concluir desde já, que o legislador optou pela não inclusão do *Malware* no leque dos meios ocultos de obtenção de prova.

No entanto existe alguma discórdia na doutrina portuguesa visto que existem autores, como nós, corroboram que não existe consagração legal da aplicabilidade do *Malware* como meio oculto de obtenção de prova e que por isso é fundamental proceder-se a uma nova alteração legislativa no âmbito do direito processual penal que considere este novo meio de obtenção de prova. Em sentido contrário, existem outros autores que, apesar de concordarem com o facto de que atualmente não existe uma norma habilitante que confira estatuto ao *Malware* como meio de obtenção de prova, socorrem-se de vários artigos consagrados na LC,[52] afirmando que podemos subsumir nestes artigos a aplicação do *Malware* como meio de obtenção de prova.

Neste sentido é importante destacar, algumas destas posições doutrinais que existem e os respetivos fundamentos. Existem autores[53] como PAULO PINTO DE ALBUQUERQUE, que defendem a aplicação do *Malware* como meio oculto de obtenção de prova, por aplicação do art.º 15.º da LC. Este autor vem afirmar que

[51] Com fundamento na expressão "recolha, em tempo real, de dados de tráfego" no art.º 20.º e no art.º 21.º da Convenção "interceção de dados de conteúdo (…) em tempo real". p.19. *ibidem.* [52] Atento o art.º 15.º, 18.º e o n.º 2 do 19.º.
[53] Como FRANCISCO MARCOLINO DE JESUS.

poderíamos subsumir a aplicação do *Malware* como meio oculto de obtenção de prova a este artigo com fundamento na expressão "pesquisa em sistema informático"[54] mas, é preciso dizer que esta pesquisa não tem necessariamente de ser realizada remotamente, tal como acontece com o *Malware*. Esta pesquisa pode muito bem ser realizada física e presencialmente, pelo que não será fundamento suficiente para tal subsunção. No entanto PAULO PINTO DE ALBUQUERQUE[55], afirma que em todo o caso, seria sempre inconstitucional, pois estamos na presença de uma clara violação do n.º 1 e 2 do art.º 26.º e, do n.º 4 do art.º 34.º da CRP, considerando que se trata de uma intromissão na privacidade do sujeito alvo visado e totalmente desproporcional, pois o art.º 15.º da LC iria permitir ao OPC utilizar o *Malware* sem controlo jurisdicional do JIC.

Existem outros autores, como: Rita Castanheira Neves, Paulo Dá Mesquita que não concordam com a subsunção ao art.º 15.º da LC ou a qualquer outro artigo que exista no nosso ordenamento jurídico considerando que não existe nenhuma norma habilitante e, por isso, não se deve aplicar o *Malware* como meio oculto de obtenção de prova em caso algum. RITA CASTANHEIRA NEVES[56], defende que nos termos do art.º 15.º não é permitida a realização de buscas online num sistema informático, sem o conhecimento do sujeito que tenha acesso àquele sistema, para recolha de dados informáticos e, portanto, nunca poderá ser permitida a utilização do *Malware* com fundamento neste preceito legal. Além do mais, o n.º 1 do art.º 15.º da LC exige que a autoridade judiciária esteja presente quando se está a realizar uma pesquisa num sistema informático, logo seria inviável a subsunção da utilização do *Malware* neste preceito legal porque colocaria em causa a ocultação deste meio.

[54] Com base no n.º 1 do art.º 15.º da LC, *in* RAMALHO, DAVID SILVA (org.). Coletânea de Legislação sobre Cibercrime e Prova Digital. P. 15. AAFDL EDITORA, janeiro 2021.

[55] *In* BATISTA, JORGE LYDIE. *O Malware como Meio de Obtenção de Prova em Processo Penal.* pp.126-127. Dissertação de Mestrado, 2018.

[56] *In* NEVES, RITA CASTANHEIRA. *As ingerências nas comunicações eletrónicas em processo penal: Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova.* pp.272 e 273. Coimbra Editora, 2011.

Na senda do que é reiterado por aquela autora, JOÃO CONDE CORREIA[57] defende que a lei atualmente não tem consagração expressa para a utilização deste instrumento, mas afirma que podem existir duas interpretações para esta situação. A primeira, assente na aplicação do n.º 5 do art.º 15.º da LC[58] pese embora estejamos perante um alargamento da "pesquisa de dados informáticos", o que iria reconduzir á explicação já enunciada. A segunda interpretação surge pela aplicação do n.º 2 do art.º 19.º da LC[59] com fundamento na expressão "recurso a meios dispositivos informáticos", interpretada no sentido de possibilitar a realização de buscas online no contexto das ações encobertas. Segundo este autor, é possível desenvolver novas formas de "lutar contra formas extremas da criminalidade, que põem em perigo a manutenção do próprio Estado de Direito"[60].

PAULO DÁ MESQUITA[61], relativamente à mesma norma legal, afirma que não se deve misturar as duas realidades porque neste preceito, pese embora a sua epigrafe, continua a remeter para a aplicação do art.º 174.º do CPP, pelo que não existe espaço para a instalação e utilização do *Malware,* nos termos do art.º 15.º da LC.

Ainda sobre esta discussão doutrinária, DAVID SILVA RAMALHO[62], provavelmente o autor que mais tem abordado e discutido esta temática na nossa doutrina, vem reconhecer a necessidade de combater o surgimento de novos programas informáticos, novas técnicas digitais que dificultam a recolha de prova no âmbito de uma investigação criminal em ambiente digital. Segundo este autor já existe, no âmbito da LC, a consagração legal do *Malware* como meio de obtenção de prova, mas não expressamente, ou seja, por aplicação do n.º 2 do art.º 19.º deste diploma[63]. Porque segundo o autor, a expressão "meios e dispositivos informáticos", constante desta disposição legal, não diz respeito aos meios

[57] *In* BATISTA, JORGE LYDIE. *O Malware como Meio de Obtenção de Prova em ProcessoPenal.* pp.126. Dissertação de Mestrado, 2018.
[58] *In* RAMALHO, DAVID SILVA (org.). Coletânea de Legislação sobre o Cibercrime e Prova Digital. P. 16. AAFDL EDITORA, janeiro 2021.
[59] *Idem.* p.18.
[60] *In* RAMALHO, DAVID SILVA. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* p.352. Almedina, Coimbra, 2017, reimpressão 2019.
[61] *In* MESQUITA, PAULO DÁ. *Processo Penal, Prova e Sistema Judiciário.* P.115. Coimbra Editora, outubro 2010.
[62] *In* RAMALHO, DAVID SILVA. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* p. 338. Almedina. Coimbra, 2017 reimpressão 2019.
[63] *In idem.* p.344.

ocultos de obtenção de prova já existentes no nosso ordenamento jurídico, afastando por completo a ideia que conceba a aplicação deste instrumento noutro art.º da LC, destinado aos meios de obtenção de prova já consagrados.

Neste sentido, afirma que nunca poderíamos subsumir este instrumento ao art.º 18.º da LC[64], porque o *Malware* por definição permite o controlo dos dados, em tempo real, que são enviados desde o dispositivo eletrónico infetado até à sua receção por outrem. Nesta situação, não existe qualquer interceção de comunicação visto que o controlo destes dados foi efetuado ainda antes de serem enviados. Assim sendo, subsumir este instrumento ao regime jurídico do art.º 18.º da LC, seria reduzir o seu próprio âmbito de aplicação, porque este preceito depende obrigatoriamente da troca de comunicações para que seja efetivamente aplicado, mas a verdade é que o *Malware*, por definição, permite assistir a toda a atividade executada pelo visado, naquele exato momento, sem que ocorra efetivamente uma comunicação. No mesmo sentido, não concorda com a posição defendida por alguns autores[65], nomeadamente PAULO PINTO DE ALBUQUERQUE, que considera aplicável à utilização de *Malware,* o regime previsto no art.º 15.º da LC. Segundo aquele autor, a própria letra da lei[66] impede a aplicação deste instrumento visto que não contempla a apreensão de dados em tempo real, apenas se refere à apreensão de dados que se encontram armazenados em sistemas informáticos e, neste sentido, estaríamos uma vez mais, a limitar o âmbito de aplicação de *Malware*. Ainda sobre este preceito legal, também não podemos utilizar o n.º 5 pois estamos perante uma "extensão de pesquisa no sistema informático inicial" com o objetivo de aceder a um segundo sistema.

Apesar de concordar que a utilização de *Malware* é subsumível no art.º 19.º da LC, o autor[67] reconhece que a solução atual é insatisfatória porque não permite regular, aquele que será o meio oculto de obtenção de prova mais restritivo dos DLG consagrados na CRP e os direitos processuais no âmbito do DPP.

[64] *Cf.* Lei do Cibercrime que corresponde à Interceção de comunicações.
[65] *In* RAMALHO, DAVID SILVA. Métodos Ocultos de Investigação Criminal em Ambiente Digital. p.342 e ss. Almedina, Coimbra, 2017, reimpressão 2019.
[66] Cf. n.º 1 do art.º 15.º da LC. "(…) dados informáticos específicos e determinados, armazenadosnum determinado sistema informático (…)".
[67] *In* RAMALHO, DAVID SILVA. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* pp.351-352. Almedina, Coimbra, 2017, reimpressão 2019.

Aliás, nas palavras do próprio "a regulação deste meio de obtenção de prova não foi tao longe quanto poderia ter sido". A este respeito, importa realçar que concordamos com o autor DAVID SILVA RAMALHO em certa medida, ou seja, não concordamos que atualmente seja possível utilizar o *Malware* como meio de obtenção de prova, por aplicação do art.º 19, como afirmado, mas concordamos quando afirma que a solução atual é insatisfatória e que se deve ponderar em introduzir, finalmente, o *Malware* como meio de obtenção de prova no nosso ordenamento jurídico.

Por outro lado, AUGUSTO SILVA DIAS procura questionar as posições que defendem a subsunção do *Malware* a qualquer artigo da LC. Desde logo, a posição que defende a aplicação do art.º 15.º da LC, considerando que este preceito exclui a obtenção de dados em tempo real, algo que o *Malware* permite fazer sendo uma das suas várias utilidades, depois afirma que o art.º 18.º da LC, na sua letra, não reflete de todo a utilização do *Malware* pelo que não poderia ser aplicável. Finalmente, atendendo ao n.º 2 do art.º 19.º da LC, este autor considera que a intenção do legislador aquando da sua redação não foi incluir a utilização do *Malware*, mas pressupondo que era essa a sua intenção não respeitaria o Princípio da Reserva de Lei.

Essencialmente estas são as principais posições que existem na nossa doutrina relativamente à utilização de *Malware* como meio oculto de obtenção de prova. Todas assentam no pressuposto de que atualmente no ordenamento jurídico português não existe qualquer diploma legal, ou disposição, que contemple a utilização de tal instrumento, o que não significa que seja uma matéria pouco trabalhada e discutida pelos especialistas na doutrina, bem pelo contrário, é um assunto que já tem sido discutido há vários anos e que cada vez mais adquire um maior relevo no panorama da investigação e prevenção criminal no nosso país face às constantes modificações da criminalidade. No entanto não se exclui a possibilidade de o *Malware* ser utilizado como meio oculto de obtenção de prova no nosso ordenamento jurídico atendendo ao nosso sistema de prova. O CPP, no art.º 125.º[68], consagra o princípio da legalidade de prova, ou seja, segundo este princípio são admissíveis todas as provas não forem expressamenteproibidas por lei.

[68] Cf. Epigrafe: "Legalidade da Prova. São admissíveis as provas que não forem proibidas por lei.".

É neste sentido, que se estabelece o nosso sistema de prova, um sistema de prova livre ou de liberdade de prova, o que significa que um meio de obtenção de prova para ser admissível não precisa estar expressamente consagrado na lei, o que não pode é estar expressamente proibido por lei. Em relação à utilização deste meio oculto, ou atípico, de obtenção de prova é preciso referir que estaria sempre sujeito aos limites constitucionais e legais de admissibilidade de prova, mesmo não estando expressamente consagrado na lei. Em relação aos limites constitucionais, estão contemplados, no n.º 8 do art.º 32.º da CRP[69], reforçado pelo n.º 1 do art.º 126.º do CPP[70]. No que diz respeito aos limites legais, encontram-se explanados no art.º 126.º do CPP. Este artigo regula as provas que são absolutamente proibidas[71], ou seja, as provas que são obtidas com recurso "à tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas". Além de regular as provas absolutamente proibidas, também consagra o regime aplicável às provas relativamente proibidas[72].

Nesta lógica, PAULO PINTO DE ALBQUERQUE, considera que sempre que um meio de obtenção de prova apresente um elevado grau de intromissão na vida privada do suspeito, aquele tem de estar consagrado em lei expressa, a menos que o visado, previamente, tenha sido informado e, tenham dado o seu consentimento expresso para a prática desse meio. Em causa estão direitos que a CRP considera que podem ser limitados em situações expressamente previstas na lei[73]. No âmbito deste regime a CRP aceita uma compressão dos direitos constitucionais, mas, sempre, em proporcionalidade e terá sempre de ser exigido a favor do interesse do Estado no normal funcionamento da justiça penal portuguesa.

[69] Segundo o qual: (…) "são nulas todas as provas obtidas mediante tortura, coação, ofensa à integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações." (…).
[70] Com base neste art.º: "1 - São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas." (…).
[71] Cf. n.º 1 e n.º 2 do art.º 126.º do CPP.
[72] Atento o n.º 3 do art.º 126.º do CPP: (…) "3- Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular." (…).
[73] Cf. art.º 26.º e o n.º 3 e 4 do art.º 34.º da CRP.

Mas a verdade é que, nem todos os países são como o nosso, visto que vários países, de alguns anos a esta parte, já utilizam este instrumento como meio de obtenção de prova, mesmo que em certas circunstâncias a sua utilização esteja proibida, o que é perfeitamente compreensível, no entanto não deixa de ser um avanço quando comparado com a situação atual do nosso ordenamento jurídico. É fundamental analisar o tratamento que é dado ao *Malware,* noutros ordenamentos jurídicos, nomeadamente, nos EUA, Alemanha, Espanha, Itália e França.

A experiência norte-americana, tem sido tudo menos regular. A verdade é que sofreu alguns percalços, no que respeita à utilização do *Malware* no âmbito de uma investigação criminal em ambiente digital. Desde logo porque, muitas vezes o que se verificou foi uma revelação, que nunca deveria acontecer, da utilização deste instrumento por parte das autoridades. Esta é uma situação que nunca poderá acontecer, e é algo que não queremos ver implementado no nosso ordenamento jurídico. A partir do momento, em que o *Malware* seja utilizado como meio oculto de obtenção de prova não podem existir comunicações que revelem a sua utilização no âmbito da investigação criminal, porque iria perder utilidade. Ou seja, a principal vantagem de utilizar o *Malware* é o facto de poder ser aplicado ao caso concreto sem o consentimento, ou conhecimento, do visado. Imaginemos, v.g., o caso das escutas telefónicas, também um meio de obtenção de prova, agora suponhamos, que o seu alvo tivesse o conhecimento de que o seu telemóvel estivesse sob escuta de um OPC?! É claro que não iria revelar nada de incriminatório nas suas conversas, e mensagens de texto. Logo o que iria acontecer é que as escutas telefónicas, nesse contexto perderiam a sua utilidade colocando em risco toda a procedência da investigação, feita até aquele momento.

O mesmo iria suceder com o recurso ao *Malware*. O primeiro caso da utilização de *Malware* nos EUA, reporta-se a 1999, com recurso ao *keylooger*[74], com autorização de mandado judicial, por OPC numa investigação desenvolvida pelo FBI no âmbito da criminalidade organizada,[75] associada ao crime de jogo ilegal. Durante esta

[74] *In* p. 19 da presente dissertação de mestrado consta a definição.
[75] *In* RAMALHO, DAVID SILVA. O Uso de Malware como Meio de Obtenção de Prova em Processo Penal. p.213, Artigo de 2013

investigação descobriu-se que o suspeito tinha no seu dispositivo eletrónico, ficheiros que estavam codificados e que podiam ser muito úteis enquanto prova. Perante esta codificação, a única solução seria descobrir a palavra-passe que pudesse desbloquear aqueles ficheiros e, nesse sentido, o FBI com base no mandado conseguiu introduzir, fisicamente, esta modalidade de *Malware* no dispositivo eletrónico do suspeito com a finalidade de descobrir a *password* e enviá-la para o FBI através de ondas de radio. Com base na utilização deste *Malware* o FBI conseguiu aceder aos ficheiros anteriormente codificados e efetuar a detenção do suspeito.

Como referi, a instalação do *keylogger* foi feita fisicamente, mas percebeu-se que essa não era a solução devido às dificuldades que existiram associadas à sua instalação. Nesse sentido e, sobretudo depois do ataque de 11 de setembro de 2001, existiu a necessidade de se procurar outra forma de instalar o *Malware*, remotamente, algo que viria a acontecer no final de 2001 com o desenvolvimento do *Magic Lantern*[76], o qual viria a ser desenvolvido em 2007 no CIPAV[77] porque permitia a recolha de várias informações, v.g., o endereço IP e respetiva localização e, ainda, uma lista de programas que estivessem em funcionamento naquele momento.

No entanto só em 2011 surgem os primeiros documentos relativos à utilização deste *Malware,* bem como o seu enquadramento legal e respetivo funcionamento. Esta modalidade de *Malware* viria a ser utilizado com bastante frequência no âmbito das investigações criminais e não só pelo FBI como também por parte de outras autoridades. Pese embora os problemas que foram surgindo na aplicação deste instrumento a verdade é que contínua a ser bastante utilizado no âmbito das investigações criminais. Em 2013, existiu um novo caso em que foi solicitada a utilização do *Malware*, contudo essa solicitação foi negada pelo Juiz da Divisão de

[76] O que se pretendia era um *keylogger* que podia ser instalado remotamente via internet, dentro ou fora do território norte-americano.
[77] *In* RAMALHO, DAVID SILVA. O uso de Malware como Meio de Obtenção de Prova em Processo Penal. p.214, Artigo de 2013.

Houston do Tribunal do Distrito do Texas[78], justificando que o processo de instalação do *Malware,* não estava devidamente fundamentado existindo a incerteza relativamente ao facto de esta modalidade de *Malware* podia invadir outros sistemas informáticos que não apenas o do visado.

Em relação à realidade europeia a análise centra-se fundamentalmente, com já enunciado, em quatro países. A Alemanha devido à influência do ordenamento jurídico alemão no nosso próprio sistema jurídico e a Espanha, devido à proximidade territorial com Portugal, e ainda, Itália e França. No ordenamento jurídico alemão, o primeiro surgimento do *Malware* numa investigação criminal remonta a 2006, no âmbito de um caso de terrorismo. Neste caso, o mandado judicial solicitado, assentava na realização de uma pesquisa remota ao dispositivo eletrónico do suspeito por intermédio do cavalo de troia[79]. Mais tarde este mandado seria recusado, existindo um recurso para o Tribunal de Justiça Federal da Alemanha, com o fundamento da analogia de outros preceitos legais do CPP alemão[80], o qual viria a ser aceite. No final de 2006, depois desta decisão, foi alterada a Lei de Proteção da Constituição da Renânia do Norte-Vestefália que veio permitir o recurso à instituição de *Malware* que ajudasse a entidade responsável a monitorizar e analisar o conteúdo.

Em virtude desta alteração, o Tribunal de Justiça Federal pronunciou-se, em fevereiro de 2008, sobre a sua constitucionalidade[81], considerando ser um diploma inconstitucional por clara violação dos princípios de clareza e certeza legal, e de proporcionalidade que necessitava ser revisto novamente. Desta feita foram introduzidas novas alterações, v.g., a possibilidade, ainda que excecionalmente, de recorrer ao *Malware* em situações de prevenção de crimes de terrorismo.

[78] *In* RAMALHO, DAVID SILVA. O Uso de Malware como Meio de Obtenção de Prova em Processo Penal. Artigo de 2013.
[79] Cf. p.17 da presente dissertação de mestrado.
[80] Cf. buscas em locais físicos, pesquisa e apreensão documentos e de sistemas informáticos.
[81] *In* RAMALHO, DAVID SILVA. O uso de Malware como Meio de Obtenção de Prova em Processo Penal.

Em relação ao ordenamento jurídico espanhol, a situação é muito precoce, tal como se verifica em Portugal[82], o que significa que ainda não existe nenhum diploma legal que regule o uso deste instrumento como meio de obtenção de prova, apesar de na doutrina não se excluir na integra esta possibilidade. Neste sentido, ORTIZ PRADILO[83], afirma que "no contexto de uma investigação criminal – nunca com caráter exclusivamente exploratório – para a descoberta de um crime particularmente grave pode ser considerada proporcional, necessária e, como tal, livre de qualquer violação de direito e liberdades fundamentais", mas também reconhece que com o tempo, pode se proceder a uma alteração legislativa fundamentando esta possibilidade.

Ainda a este respeito importa realçar o que se verifica no ordenamento jurídico italiano e no francês. Em relação ao ordenamento jurídico italiano, a utilização deste *software* está regulada desde 2018, com a designação de *captatore informático*, no n.º 2 do art.º 266.º e ss. do código processo penal italiano. Este meio está vocacionado, no âmbito da investigação criminal, para o combate a crimes, v.g., criminalidade organizada, terrorismo, tráfico de estupefaciente. Neste contexto a sua utilização depende, obrigatoriamente, de um requerimento apresentado pelo MP, onde faça constar que os indícios da prática do ilícito criminal justificam a utilização deste meio durante determinado período e, consequentemente, não existe outro meio menos gravoso, que permita solucionar o problema em questão. Em seguida, esse requerimento terá de ser aprovado judicialmente, onde deve constar o modo de funcionamento do *software*. Em Portugal, deveríamos desenvolver uma nova lei, que tivesse por base as exigências italianas, só assim poderemos ter uma lei completa e que permita regular a utilização de *Malware* como meio de obtenção de prova.

Finalmente, em França também existe uma previsão legal que contempla a utilização deste *software*, no âmbito da investigação criminal no *code de procédure pénale*[84]*,* que apenas poderá ser aplicado aos crimes de elevado grau de risco, tal como sucede no ordenamento jurídico italiano. Todavia, em França o regime é mais

[82] *In* RAMALHO, DAVID SILVA. O uso de Malware com Meio de Obtenção de Prova em ProcessoPenal. art.º de 2013.
[83] *In* RAMALHO, DAVID SILVA. O uso de Malware como Meio de Obtenção de Prova em Processo Penal. art.º 2013.
[84] Em português, código de processo penal.

completo, pois prevê a obrigação de elaborar um relatório de operações, exatamente como acontece em Portugal no âmbito do regime jurídico das AE, sendo possível armazenar ou destruir todos os dados que foram recolhidos num determinado dispositivo eletrónico.

2.2. Ação Encoberta

Para analisar o regime jurídico das AE é importante ter em consideração dois diplomas, o RJAE[85] e a LC[86], isto é, apesar do regime aplicável às AE estar contemplado, na sua totalidade, no primeiro, a verdade é que precisamos sempre de mencionar a LC, porque é onde se encontra um artigo[87] dedicado exclusivamente às AE em ambiente digital com o objetivo de autonomizar esta modalidade de ação encoberta.

Além do mais esta autonomização também assentou noutros fatores entre eles: a redução do seu objeto, circunscrevendo-o apenas à cibercriminalidade o que acarreta dificuldades acrescidas relativamente à recolha de prova, devido ao facto de que todos os ilícitos criminais ocorrem em ambiente digital, tornando-se difícil imputar a um individuo a prática de tais crimes; a sua natureza preventiva, ou seja, se os ilícitos fossem exclusivamente cibercrimes isso significaria que a atuação do agente encoberto teria de ser realizada exclusivamente em ambiente digital, inclusive a interação com o suspeito e a recolha de prova teriam que ser feitas em ambiente digital. Como já mencionado, uma das principais dificuldades neste meio é identificar[88] o autor do ilícito criminal, tornando a atuação do agente encoberto mais difícil porque não só tem de recolher prova sobre o cometimento, ou a intenção do ilícito criminal, mas também tem de descobrir, ou tentar, a identidade real do suspeito, para que lhe possam ser imputadas as provas recolhidas.

[85] *In* Lei n.º 101/2001, 25 de agosto.
[86] Cf. Lei n.º 109/2009, 15 de setembro.
[87] Atento o art.º 19.º da LC. É com base neste art.º que alguns autores afirmam que é possível subsumir, atualmente, a utilização do Malware como meio de obtenção de prova.
[88] Pode estar a utilizar um *nickname* ou simplesmente um nome falso.

Finalmente, sempre que a recolha de prova seja possível, em ambiente físico, e com recurso a um outro meio de obtenção de prova menos gravoso, CPP ou na LC, a ação encoberta será sempre considerada desproporcional, excessiva[89].

Antes de analisar em concreto o regime jurídico das AE consagrado na lei n.º 101/2001 é fundamental referir que a sua aplicação não é pacifica, ou seja, exis- tem várias críticas a esta lei, nomeadamente, em relação ao modo como foram consagrados os preceitos legais, questionando a sua própria constitucionalidade. Uma das críticas, reporta-se à ausência de disposição legal que contemple a atuação do AE, nomeadamente, estipulando os atos que pode desenvolver na sua atividade. Outra critica, em relação ao facto de não existir um preceito normativo que exija uma revisão legal dos pressupostos consagrados na presente lei.

A mais importante de todas elas em virtude da sua gravidade diz respeito ao relatório final[90] elaborado pelo próprio AE não ter de constar dos autos no processo, ou seja, diz-nos a presente lei, que não existe obrigatoriedade de se juntar aos autos como prova, o relatório elaborado pelo agente encoberto, impossibilitando o arguido e o próprio juiz de julgamento de ter conhecimento do que foi escrito nesse relatório.

Quanto a nós, em relação às últimas duas críticas, estamos totalmente de acordo. Em relação à inexistência de norma que preveja obrigação de revisão legal dos pressupostos aplicáveis ao regime jurídico da AE, acreditamos que deveria, efetivamente, de existir uma norma que previsse essa revisão em determinados períodos, porque face à volatilidade da cibercriminalidade é necessário que a própria lei acompanhe as evoluções que surgem, nomeadamente, quanto aos meios empregues e que os pressupostos aplicados às AE sejam capazes de combater essas inovações.

[89] Como resulta do n.º 1 do art.º 3.º da RJAE: "as ações encobertas devem ser adequadas aos fins de prevenção e repressão criminais identificados em concreto, nomeadamente a descoberta de material probatório, e proporcionais quer àquelas finalidades quer à gravidade do crime em investigação." *In* RAMALHO, DAVID SILVA (org.). *Coletânea de Legislação sobre Cibercrime e Prova Digital.* AAFDL EDITORA. Lisboa, 2021.

[90] No qual se regista todos os acontecimentos e atos realizados pelo Agente Encoberto durante o período em que se levou a cabo a AE. E, por norma, terá enorme valor probatório para a acusação.

No que diz respeito à última crítica apresentada, sobre a não obrigatoriedade de inclusão do relatório nos autos do processo, apesar da fundamentação utilizada pelo legislador[91], é uma clara violação dos direitos do arguido, nos termos do art.º 32.º da CRP, visto que o arguido tem o direito de conhecer todas as provas que a acusação tem contra si, bem como o que originou a presente acusação e o relatório elaborado pelo AE, regra geral, terá um enorme valor probatório, pelo que consideramos que deveria ser obrigatória a sua junção aos autos do processo. Neste sentido o Ac. do STJ, processo n.º 326/12.0JELSB.L1.S1, de 10 de março de 2016[92] vem corroborar o exposto no art.º 4.º da RJAE, afirmando com a devida ressalva neste preceito legal, que "o relato da ação encoberta, em si, enquanto documento descritor daquilo a que o agente assistiu não tem valor probatório apesar do art.º 471.º da Lei n.º 101/2001, inculcar a ideia de que é possível utiliza-lo em termos probatórios se isso for absolutamente indispensável".

No que diz respeito à primeira crítica apresentada, aí já não concordamos, porque a existir uma norma que regulasse os atos a executar pelo AE no exercício da sua atividade, isso seria o mesmo que limitar a sua própria atuação, ou seja, os casos em que a AE é autorizada são dos mais variados e não deve ficar o AE limitado às especificidades que essa norma iria acarretar. A atuação do AE está limitada, desde logo, ao princípio da proporcionalidade, da necessidade e ainda será sempre vigiada pela AJ, logo não faz sentido estar a limitar ainda mais a sua atividade. Além do mais, é o AE que estabelece uma relação com o suspeito e que tem um contacto privilegiado com a prática do crime, logo deverá ficar ao seu livre-arbítrio, salvo as limitações já elencadas, realizar todas as ações que se mostrem necessárias para atingir o sucesso da AE.

Em relação ao regime jurídico propriamente dito, diz-nos o n.º 1 do art.º 19.º da LC,[93] que "é admissível o recuso às ações encobertas previstas na Lei n.º 101/2001, de 25 de agosto, nos termos aí previstos (…)", o que nos leva a concluir

[91] Cf. veremos em seguida, a finalidade é proteger a verdadeira identidade do AE, mas a verdadeé que existem formas para combater esta possibilidade, que não esta.

[92] *In* Acórdão do Supremo Tribunal de Justiça (dgsi.pt)

[93] *In* RAMALHO, DAVID SILVA (org.). *Coletânea de Legislação sobre o Cibercrime e Prova Digital.* AAFDL EDITORA. Lisboa, 2021.

que o regime aplicável às AE em ambiente digital, é o mesmo que encontramos no RJAE, aplicado às AE em ambiente físico. A principal diferença será o âmbito de aplicação, visto que as ações encobertas em ambiente digital só são aplicáveis aos crimes consagrados na própria LC, ou então "os crimes cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior (…) os crimes contra a liberdade e autodeterminação sexual (…), a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras (…)"[94], ao passo que o âmbito de aplicação das AE em ambiente físico é mais amplo[95].

Atendendo ao n.º 1 do art.º 19.º da LC, o regime jurídico em análise será o que consta do RJAE. Assim sendo, o primeiro aspeto relativo ao regime jurídico das AE é a criação de uma identidade fictícia[96], com fundamento no disposto no n.º 1 do art.º 5.º do RJAE[97], o que significa que, os OPC podem desenvolver a sua atividade assente numa identidade que não a sua identidade real. Esta identidade só pode ser atribuída através de despacho do MJ depois de proposta pelo diretor nacionalda PJ[98].

Todavia esta identidade não pode existir intemporalmente, por isso a lei estabelece um período de seis meses, o qual pode ser renovável por um período igual[99], e apenas poderá ser utilizada "no exercício da concreta investigação quer em todas as circunstâncias de tráfico jurídico e social"[100]. Se atendermos às ações encobertas em ambiente digital, a criação de uma identidade fictícia implica a

[94] Al. a) e b) do n.º 1 do art.º 19.º da LC. *In* RAMALHO, DAVID SILVA (org.). *Coletânea de Legislação sobre o Cibercrime e Prova Digital.* AAFDL EDITORA. Lisboa, 2021.
[95] Cf. o art.º 2.º do RJAE. *Idem.*
[96] Atento o faco de ser subsumível às duas modalidades de AE. No caso das ações encobertas em ambiente digital importa referir que esta identidade fictícia é num ambiente online através da criação de *username* ou *nickname*.
[97] Segundo o qual "Para efeito do n.º 2 do art.º 1.º, os agentes de polícia criminal podem atuar sob identidade fictícia". *In* RAMALHO, DAVID SILVA (org.). *Coletânea de Legislação sobre Cibercrime e Prova Digital.* AAFDL EDITORA. Lisboa, 2021.
[98] Nos termos do n.º 2 do art.º 5.º do RJAE. *Idem.*
[99] Cf. primeira parte do n.º 3 do art.º 5.º do RJAE. *Idem.*
[100] Cf. segunda parte do n.º 3 do art.º 5.º do RJAE. *Idem.*

criação de um perfil no *facebook*[101] com o objetivo de estabelecer comunicação com os suspeitos como o agente encoberto se identificam da mesma forma. Neste sentido, o nome fictício do agente convém já estar anteriormente inserido no meio que este se pretende integrar.

O principal objetivo desta criação não é enganar, ludibriar, as pessoas com quem se mantém contacto, mas fundamentalmente proteger a segurança do próprio AE, para que não haja futuras represálias contra si, ou contra a sua família. Neste sentido, poderá atuar constantemente com outra identidade, aparentemente real, em todos os momentos da sua vida, pelo menos até ao término da AE. Deste modo o agente se tiver de estabelecer contacto com o possível suspeito não terá de utilizar o seu nome real para se identificar.

Por norma, esta realidade é muito frequente porque o agente encoberto na sua atuação, tem de entrar em contacto com o possível suspeito o que pode gerar desconforto ou, inclusive, medo no agente encoberto especialmente se estivermos no âmbito das AE em ambiente físico, que normalmente implicam um contacto direto, físico e visual. No entanto, o estabelecer contacto não implica, obrigatoriamente, que o suspeito vá descobrir a verdadeira identidade do AE, mesmo porque não terá motivos para desconfiar pois todas as informações sobre este serão credíveis, apesar de serem todas falsas. A verdade é que quanto menor for o contacto entre as partes melhor, a menos que se revele fundamental para a recolha de prova. Em sentido contrário, se estivermos no âmbito das AE em ambiente digital o risco, falado anteriormente, torna-se praticamente nulo, porque o contacto, é realizado online, podendo o agente estar em qual- quer local do mundo, utilizar um *username*, e assim, torna-se quase impossível ser descoberto. Além do mais, o contacto físico, que referíamos, é praticamente inexistente, porque é tudo realizado através de um dispositivo eletrónico.

[101] Inclusive noutra rede social que seja necessário para o sucesso da atuação do agente encoberto, preenchendo todos os campos exigidos ainda que com informação falsa, obviamente. Esse perfil não poderá transmitir desconfiança a terceiros, pelo que tem de ser o mais vulgar possível.

Apesar do período regulado no n.º 3 do art.º 5.º do RJAE, a verdade é que esta identidade pode ser utilizada, excecionalmente, fora do âmbito das AE, sempre e desde que estejamos numa fase mais adiantada da investigação, v.g., se estivermos no âmbito de um julgamento ou audiência final. Pode dar-se a situação do agente encoberto ter de testemunhar na presença do arguido e, nessa situação por razões óbvias de segurança, o agente pode manter a sua verdadeira identidade no anonimato ou, uma segunda alternativa, será o juiz de julgamento decretar que o depoimento prestado seja ouvido cf. o regime jurídico aplicado à proteção de testemunhas[102].

É importante referir, para não existir dúvidas, que esta é a única situação possível em que o agente pode permanecer com a sua identidade fictícia fora do âmbito da sua atuação enquanto AE. A criação de uma identidade fictícia, depois de autorizada pela AJ, tem de estar sujeita a limites, isto é, não pode ficar ao livre-arbítrio do agente para que possa escolher um nome qualquer que pretenda. Além do mais, terá de existir um limite máximo ao número de *nicknames* que o agente pode utilizar no âmbito da sua atuação.

Pretende-se assim evitar a escolha de nomes excessivos, ou demasiadamente sugestivos, isto porque o nome escolhido pode instigar, provocar, o suspeito a cometer um ilícito criminal, depois de estabelecer contacto com o agente encoberto, o que recairia automaticamente no âmbito da figura do agente provocador e, como já vimos, trata-se de uma figura absolutamente proibida no âmbito do processo penal português. Depois de criada essa identidade, o agente deve comunicar à AJ o nome escolhido para que possam controlar, a todo o momento, a atividade desenvolvida pelo agente.

Pode dar-se a situação de que o nome escolhido já exista e pertença a um outro individuo envolvido no ambiente em que o AE pretendia integra-se, levantando assim uma nova questão, a de saber se o AE pode, ou não, utilizar um nome que anteriormente foi utilizado por alguém envolvido no meio criminoso que se pretende integrar, e além disso, o que irá acontecer à prova recolhida.

[102] Cf. Lei n.º 93/99 de 14 de julho conhecida como a Lei de Proteção de Testemunhas.

Nesta situação tudo depende da legitimidade com que o agente se apoderou de tal nome, ou seja, se aquele nome foi voluntariamente entregue pelo seu usuário, se o agente obteve de forma legal, então nada o impede de utilizar durante a sua investigação o que facilita, e muito, a sua atuação visto que a relação de confiança que normalmente se estabelece com o suspeito já não é preciso ser conquistada porque pressupõe que já existe entre o terceiro e o suspeito, com a diferença que, no caso concreto, o suspeito não tem conhecimento que já não está a falar com aquele, mas sim com o agente encoberto disfarçado de terceiro.

Neste caso, obviamente que a prova recolhida será validada. Em sentido contrário, estão as situações em que o agente simplesmente se quer aproveitar da relação de confiança, anteriormente estabelecida e, para o efeito, usurpa a identidade do terceiro. Outro aspeto muito importante a destacar no regime jurídico das ações encobertas é a isenção de responsabilidade[103] que o AE goza no exercício da sua atuação, ou seja, a regra é da irresponsabilidade do agente na sua atuação[104], a menos que a intervenção do agente na prática do crime se consubstancie numa autoria mediata ou instigação[105] e, nestas situações, o agente será responsabilizado pela sua atuação.

No entanto, existem algumas situações, muito excecionais, que permitem ao AE atuar em autoria material, cf. EDUARDO MAIA COSTA[106], ou seja, segundo este autor, se o sucesso da investigação estiver em risco, bem como a falsa identidade, será admitido ao AE a prática de ilícito criminal sob autoria material, mas sempre no pressuposto de que estejam preenchidos, não só o princípio da proporcionalidade, mas também o princípio da necessidade.

[103] Cf. art.º 6.º do RJAE. *In* RAMALHO, DAVID SILVA (org.). Coletânea de Legislação sobre Cibercrime e Prova digital. AAFDL EDITORA. Lisboa, 2021.
[104] Com base no disposto na primeira parte do n.º 1 do art.º 6.º do RJAE: "Não é punível a condutado agente encoberto (…)". *Idem.*
[105] Cf. segunda parte do n.º 1 do art.º 6.º do RJAE: "(…) em qualquer forma de comparticipação diversa da instigação e da autoria mediata (…)". *Idem.*
[106] RAMALHO, DAVID SILVA. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* p.307. Almedina, Coimbra. 2017, reimpressão em 2019.

Contrariamente a esta posição, surge RUI PEREIRA,[107] afirmando perentoriamente que o AE é sempre proibido, quando o seu envolvimento no cometimento de crimes não aconteça no âmbito da comparticipação.

O último ponto a abordar nesta temática é o relatório do agente encoberto[108], que surge no final da sua atuação e serve para o AE descrever pormenorizadamente tudo o que aconteceu e realizou durante aquele período, como sabemos é pelo menos seis meses sendo renovável. A principal questão nesta matéria, assenta no facto do relatório não ser junto aos autos do processo, ou seja, segundo o art.º 4.º do RJAE, não existe obrigatoriedade do relatório, elaborado pelo AE no fim da sua atuação, ser junto aos autos a menos que "(…) se a reputar absolutamente indispensável em termos probatórios"[109]. Neste contexto, o Ac. do STJ, supramencionado[110], afirma que o relato da AE pode não ser tido em consideração como meio de prova em sede de audiência de julgamento. No caso em apreço, não foi visto que já tinha sido admitida como prova testemunhal, o testemunho do "agente infiltrado ele melhor do que ninguém poderia esclarecer os contornos da ação encoberta".

Pese embora, as razões que fundamentam esta opção sejam válidas de extrema importância, DAVID SILVA RAMALHO discorda com a posição adotada pelo legislador, de tal modo, que a considera inconstitucional por violação do n.º 1 do art.º 32.º da CRP[111]. A opção tomada pelo legislador, assenta fundamentalmente na garantia de segurança do próprio agente encoberto, ou seja, pretende-se evitar o risco de o arguido descobrir a verdadeira identidade do AE, durante esta fase do processo, causando danos quer ao próprio, quer à sua família. O que este autor nos vem dizer, é que as ações encobertas não são todas perigosas, especialmente se estivermos no âmbito das AE em ambiente digital e, consequentemente, não acarretam aquele risco. Além do mais é possível o AE ser

[107] *Idem.*
[108] Cf. art.º 4.º do RJAE. *In* RAMALHO, DAVID SILVA (org.). Coletânea de Legislação sobre Cibercrime e Prova digital. AAFDL EDITORA. Lisboa, 2021.
[109] Cf. parte final do n.º 1 do art.º 4.º do RJAE. *Idem.*
[110] Cf. p. 46 da presente dissertação de mestrado.
[111] Cf. "o processo criminal assegura todas as garantias de defesa, incluindo o recurso" *in* ::: Decreto de 10 de Abril de 1976 (pgdlisboa.pt).

substituído durante a sua atuação, sempre que a sua identidade esteja em risco de ser descoberta, por um colega sem que o suspeito se aperceba de tal mudança, visto que o substituto continuará a utilizar o mesmo *username,* a mesma identidade fictícia do agente inicial.

Se estivermos no âmbito das AE em ambiente digital, o risco de descobrimento da identidade real do agente encoberto é praticamente nulo, visto que a relação que se estabelece entre o AE e o suspeito é fundamentalmente virtual e impessoal, o que dificulta ainda mais ao suspeito descobrir a identidade do agente encoberto, pelo que, nestas situações em que o risco é diminuto o relatório elaborado pelo AE deve ser junto aos autos.

Ainda sobre as ações encobertas, como referido inicialmente, é fundamental identificar as diferenças que existem entre as duas modalidades de AE, quer em ambiente físico, quer em ambiente digital. Pese embora existam semelhanças, entre estas duas modalidades, que permitem desde logo a aplicação do regime jurídico do RJAE nas ações encobertas em ambiente digital, a verdade é que existem várias diferenças entre si, principalmente em termos práticos, ou seja, a própria atuação do agente encoberto não é a mesma em ambiente digital, do que aquela que tem em ambiente físico.

Estas diferenças surgem principalmente do ponto de vista da atuação do agente encoberto. Em primeiro lugar, a criação de uma identidade fictícia em ambiente digital permite ao AE utilizar várias identidades ao mesmo tempo em vários fóruns estabelecendo várias relações com múltiplos suspeitos, algo que não é possível de acontecer no ambiente físico. Além do mais, os riscos a que o agente encoberto está sujeito são mínimos, quase nulos, em ambiente digital quando comparado com a sua atuação no ambiente físico, visto que a relação que se estabelece entre o agente e o suspeito não obriga a um contacto físico, visual, dificultando ainda mais, a capacidade do suspeito de descobrir a verdadeira identidade do agente encoberto. Associado a este risco importa referir, que em ambiente digital, um erro cometido pelo AE não implica necessariamente consequências para a sua segurança, pelos motivos já elencados, ao passo que, em ambiente físico o agente encoberto não pode errar, porque um simples erro pode ser crucial para colocar

em risco toda a sua investigação, bem como a sua própria segurança e a da sua família.

Em ambiente digital, o AE não precisa estar num local físico para executar a sua atividade, aliás, pode estar na sua própria residência ou no seu gabinete. Em ambiente digital, existe um risco maior de o agente encoberto atuar com o objetivo de atingir um benefício próprio praticando ilícitos que não tem qualquer relação com a sua atividade ou então, instigar a prática de crimes com a identidade que criou e, com uma segunda identidade, recolher a prova desse mesmo crime com o objetivo de atingir o sucesso da sua investigação. Tudo isto é possível, porque se pode aproveitar das tecnologias anti forenses[112], visto que estas podem ser utilizadas como forma de garantir o anonimato na internet.

As medidas anti-forenses podem ser divididas em dois grandes grupos[113]: medidas anti forenses para evitar a deteção e, as medidas anti forenses para evitar o exame e a análise de dados informáticos. Aquele primeiro grupo, subdivide-se em anonimizadores, e as moedas virtuais, v.g., bitcoin. O segundo grupo, subdivide-se na eliminação de dados, na dissimulação de dados e, ainda, a adulteração de dados. Este risco associado ao ambiente digital obriga a AJ, a ter um controlo apertado sobre a atuação do AE, exigindo-lhe um registo obrigatório de toda a sua atividade, no âmbito das ações encobertas com o objetivo de evitar que se verifiquem situações, como as já elencadas.

[112] " *In* RAMALHO, DAVID SILVA. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Pp. 150-151. Reimpressão 2019, Coimbra. Almedina. Definido por BURKHARD SCHAFER e STEPHEN MASON como sendo "qualquer técnica, ferramenta de hardware ou software que previne ou atrasa a análise forense de um suporte de dados e afeta negativamente a existência, quantidade, autenticidade ou qualidade da prova de um computador". Ou seja, permitem "frustrar a deteção, monitorização, prova ou imputação de uma determinada atividade em ambiente digitalao seu autor".
Definido como "técnicas e/ou programas informáticos que ocultam a identidade de um individuo e a informação por ele transmitida ou a ele enviada via telecomunicações, bem como os dados armazenados num sistema informático ou dispositivo eletrónico" *in in* RIBOLI, EDUARDO BOLSONI. *A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a intercetação de comunicações em massa e os softwares de espionagem.* P.3. Galileu – Revista de Direito e Economia, volume XIX, 1 de julho a 31 de dezembro de 2018.
[113] *Idem.* p.16.

Posto isto, torna-se clara a necessidade de uma alteração legislativa no sentido de introduzir, no processo penal português, o regime jurídico das ações encobertas em ambiente digital. Estamos na presença de duas realidades bem distintas, do ponto de vista prático, visto que a realidade digital é bem mais complexa que a realidade física. Logo esta tentativa de aplicar o regime jurídico consagrado no RJAE, às ações encobertas em ambiente digital torna-se muito difícil de executar no caso concreto porque este regime será insuficiente para regular todas as situações possíveis no mundo digital.

No caso concreto, este regime jurídico demonstrará insuficiência em regular aspetos específicos do mundo digital, que não acontecem no mundo físico, e sempre que estivermos perante um caso que recaía no âmbito do art.º 19.º da LC e que não tiver comparativo no mundo físico, irá existir um "buraco" que será preenchido por soluções inadequadas ao caso concreto, com base na experiência ou no senso comum. Neste sentido, estaríamos perante uma analogia, proibida em direito penal. Importa referir que não estaríamos a introduzir um novo meio oculto de obtenção de prova, mas sim atribuir um maior relevo a esta modalidade de AE, porque atualmente a cibercriminalidade tem vindo a aumentar e a tendência no futuro, será a de continuar a aumentar. Como já vimos, existem várias diferenças entre estas duas modalidades de AE, que torna o atual regime jurídico insuficiente quando pretendemos aplicar às ações encobertas em ambiente digital.

Atualmente não se distingue as AE em ambiente físico, das AE em ambiente digital, o que se verifica não só no ordenamento jurídico português como também noutros ordenamentos jurídicos[114], principalmente devido à falta de base legal no que toca às ações encobertas em ambiente digital.

[114] *In* RAMALHO, DAVID SILVA. Métodos Ocultos de Investigação Criminal em ambiente digital. 2017 p.283. Segundo DAVID SILVA RAMALHO, depois de fazer uma pesquisa intensiva, para o seu livro, noutros ordenamentos jurídicos verificou que também não existe numa disposição legal que preveja, em concreto, a aplicação de um regime jurídico próprio à AE em ambiente digital.

Em compensação, recorre-se ao regime jurídico consagrado no RJAE para dar resposta à cibercriminalidade. A AE em ambiente digital é, tendencialmente, observada como uma modalidade, ou vertente, da AE em ambiente físico e, nunca, como um novo meio oculto de obtenção de prova, visto que a principal semelhança é a ocultação, ativa ou passiva, da real identidade do AE, que normalmente é acompanhada de uma comunicação com terceiros, estabelecendo uma relação de confiança com aquele, através da falsa identidade. A ocultação será ativa sempre que o agente intencionalmente decide não divulgar a sua verdadeira identidade e cria uma identidade fictícia e, contrariamente, a ocultação será passiva sempre que o agente se limite a não responder a questões pessoais ou, em situações em que não seja questionado sobre a sua verdadeira identidade, mas seja presumida por terceiros.

3. DARKWEB

No nosso ordenamento jurídico, em concreto na LC, existem algumas falhas no que concerne à utilização dos meios de obtenção de prova no âmbito de uma investigação criminal no âmbito da D*arkWeb.* Neste sentido procuramos não só esclarecer alguns conceitos, v.g., *DarkWeb, DeepWeb* e *SurfaceWeb*, distinguindo-os entre si, e elencar alguns programas de software que permitam aos utilizadores aceder à *DarkWeb*, à *DeepWeb*, nomeadamente a *freenet* e o *tor*. A referência às criptomoedas, principalmente, a *bitcoin*, em virtude de serem utilizadas em transações online no âmbito de ilícitos cibernéticos. Por último, pretendemos analisar os meios de obtenção de prova consagrados na LC e verificar se são suficientes e eficazes para o sucesso da investigação criminal na *DarkWeb,* bem como a relevância da AE neste contexto.

3.1. Diferenças em relação à *DEEPWEB* e à *SURFACEWEB*: Programas de Software e Criptomoedas

Para distinguir estes três conceitos, nada melhor do que nos socorrermos da seguinte frase "se imaginarmos um icebergue, dividido horizontalmente em três partes, em que a central será maior do que a parte superior e a parte inferior, poder-se-á referir à nossa conhecida internet (também conhecida por *Surface-Web*) no topo, como aquela parte que está acima do nível da água, a *DeepWeb*, a baixo do nível da água até uma profundidade considerável, e na parte inferior e mais escura, a *DarkWeb*".[115] Desta frase podemos concluir, que a única semelhança entre estes conceitos é o facto de todos eles serem "camadas" da internet, ou da *Web*, conceito que igualmente merece esclarecimento[116]. A *WEB* subdivide-se naqueles três níveis[117], sendo a *SurfaceWeb* o primeiro nível, a *DeepWeb*, é o segundo nível e, finalmente, no terceiro nível a *DarkWeb*, aquele cuja acessibilidade é mais difícil.

No que diz respeito à *SurfaceWeb*[118], é a área da web que o utilizador, normalmente, tem acesso todos os dias, bem como ao seu conteúdo, podendo aceder através dos motores de busca tradicionais[119]. Fundamentalmente é a zona da internet que qualquer utilizador, inclusive aqueles com diminutas capacidades informáticas, pode aceder sem qualquer problema. Em sentido contrário a *DeepWeb,* camada imediatamente abaixo, engloba toda a informação que não pode ser obtida livremente, cujo acesso é considerado indisponível para o normal utilizador, isto é, com falta de conhecimentos técnicos.

[115] *In* SCHWALBACH, JOSÉ GASPAR. *Direito Digital.* P.29. Almedina, Coimbra, 2021.

[116] A *Web* é um sistema de informações conectadas entre si com base em hiperligações que concedem aos seus utilizadores acesso a uma panóplia de conteúdos socorrendo-se da internet, nomeadamente, de um *browser.*

[117] A distinção entre estes três conceitos será realizada pela ordem apresentada.

[118] *In* SILVA, ANDRÉ TIAGO RIBEIRO. *As Ações Encobertas à Luz do Processo Penal Português*. Dissertação de Mestrado em Direito e Prática Jurídica, especialidade em Ciências Jurídico-Forenses. FDUL, 2019.

[119] V.g. *google chrome, safari*, *Firefox* ou *internet explorer*. A este respeito, e a título de curiosidade, apenas 16% da informação que existe na internet (englobando todas as camadas), pode ser acedida através destes, e de outros, motores de busca tradicionais, como por exemplo, Facebook, Amazon e Netflix. A restante informação encontra-se dispersa na *DeepWeb* e na *DarkWeb*.

Não podemos aceder a este nível da internet através dos motores de busca tradicionais[120], teremos sempre de socorrer-nos de endereços próprios, e a partir de sistemas de autenticação[121], visto que na *DeepWeb*, encontramos informação de enorme qualidade e relevância quando comparada com a informação que facilmente encontramos na *SurfaceWeb*.

Na esmagadora maioria dos sites que se acede utilizam caches[122] permitindo recolher informações pessoais do utilizador com o objetivo de melhorar a sua experiência no site, caso no futuro volte a entrar. No entanto, é preciso referir que continua a existir muita informação que os seus utilizadores não têm acesso, porque se encontra vedada à última camada da *Web*, a *DarkWeb*, e os motores de busca utilizados não estão programados para executar pesquisas mais profundas nos servidores da internet. Os utilizadores quem tem acesso a este nível da internet já conseguem executar ilícitos criminais, tais como, tráfico de armas[123] e drogas, pedofilia. Neste contexto, as criptomoedas que mais são utilizadas para realizar transações online neste meio é a bitcoin. Como último nível da internet, encontramos o conceito de *DarkWeb*, o qual não pode ser confundido com outro conceito, a *DarkNet*. Este diz respeito a uma rede virtual criada por vários utilizadores, de acesso restrito aos não criadores, operada na internet com o intuito de compartilhar informações e ficheiros sob formato digital e, ao mesmo tempo, impossibilita a descoberta, quer do endereço IP[124] de cada membro, bem como de todo o conteúdo das suas comunicações.

[120] *In* SILVA, ANDRÉ TIAGO RIBEIRO. *As Ações Encobertas à Luz do Processo Penal Português*. Dissertação de Mestrado em Direito e Prática Jurídica, especialidade em Ciências Jurídico-Forenses. FDUL, 2019.

[121] V.g. banco de dados corporativos, portais dedicados unicamente aos alunos, ou ainda, as plataformas de venda e-commerce.

[122] Funcionam como um depósito de informações guardadas em compartimentos do sistema operacional, quer seja em smartphones ou computadores. Este depósito permite que o sistema utilize esses dados de uma forma mais rápida e eficaz. O cache funciona como um armazém temporário sendo constantemente abastecido com novos dados e informações.

[123] Segundo o IOCTA de 2020, o tráfico de armas tornou-se "mais fragmentada". *In* IOCTA (2020): versão original. EUROPOL. Internet Organised Crimes Threat Assessment. 2020.

[124] Ou protocolo de internet, assente num conjunto de regras que nos indicam como os dados informáticos tem de ser entregues, com recurso à rede pública. Este protocolo existe em todos os dispositivos eletrónicos que estejam ligados à rede para a transmissão de dados e permite determinar o local em que o utilizador se encontra quando esta a tentar aceder ao dispositivo eletrónico, ou ainda, o local em que se encontra quando recebe ou envia fotos durante uma conversa, no Facebook, Instagram, WhatsApp, etc. *In* SCHWALBACH, JOSÉ GASPAR. *Direito Digital.* P.34. Almedina, Coimbra, 2021.

Em sentido contrário aquele conceito reporta-se à zona "mais escura, mais profunda" da internet e à qual não podemos entrar pela Internet, em virtude da falta de determinados softwares, configurações ou autorizações que permitam ao utIzador ter acesso à *DarkWeb*. Por outras palavras, é um conceito que apresenta uma conotação assente no facto de que existem dados, ficheiros informáticos que estão armazenados num local da *Web* inacessível à maioria dos utilizadores, ou pelo menos acreditam que não conseguem aceder. Não existe informação que não seja possível aceder, porque com os conhecimentos técnicos necessários e utilizando a ferramenta correta é possível ao utilizador aceder a qualquer informação que se encontre na *Web*, independentemente da camada. Agora se utilizarmos, por exemplo, os motores de busca tradicionais então existe uma panóplia de informação, à qual nunca teremos acesso.

O acesso à *DarkWeb* só será possível mediante a utilização de determinados programas informáticos, v.g. *freenet* ou *tor*[125]. Quando comparamos os três níveis da internet é fácil compreender que a *DarkWeb*, é aquela que exige um acesso mais restrito à informação e onde conseguimos, normalmente, comprar e vender todo a variedade de produtos[126], sem nenhum controlo e claramente ilícitos, não só drogas, armas, e ainda, contratos de assassinatos, informações confidenciais, entre outros. Relativamente à prática de cibercrimes, no âmbito da *DarkWeb,* podemos referir entre eles: o tráfico de droga[127], a exploração infantil, os contratos de assassinatos, o tráfico de seres humanos e, ainda, a publicação de vídeos reais demonstrando práticas de tortura até à morte.

A este respeito importa evidenciar dois autores: *OWEN, GARETH* e *MOORE, DANIEL*[128]. Segundo o primeiro autor, em 2015, os serviços disponíveis diziam respeito às apostas, venda de armas, abusos, pornografia, *hacking*, contrafação, denúncias, fraude, entre outros. O segundo autor, vem nos dizer que no inicio de

[125] Veremos o que significam já em seguida, no subtítulo.
[126] Cf. *SILK ROAD* (ou rota da seda), criado em fevereiro de 2011, sendo um dos mercados de venda de produtos ilegais na *Dark Web*. Não conseguiremos aceder a este mercado através dos motores de busca tradicionais. Temos de utilizar o browser *TOR*. Durante muitos anos este foi um dos maiores mercados de droga. Este mercado em 2015 foi derrubado pelo FBI e o seu criador, no mesmo ano, foi condenado a prisão perpétua. P.30 *idem.*
[127] Atendendo ao *IOCTA* de 2020, as drogas mais pesadas são: opioides, fentanil e a heroína. *In* IOCTA (2020): versão original. EUROPOL. Internet Organised Crimes Threat Assessment. 2020. [128] *In* SCHWALBACH, JOSÉ GASPAR. *Direito Digital.* P.30. Almedina, Coimbra, 2021

2016, os serviços prestados reportavam-se ao extremismo, pornografia, serviços financeiros ilícitos, venda de produtos estupefacientes, entre outros. Nestes termos, estabelecendo uma comparação entre a *Deep* e a *DarkWeb*, podemos afirmar que embora apresentem a mesma estrutura, visto que é impossível aceder a ambas através dos motores de busca tradicionais, v.g., *google.chorme* ou *internet explorer*, a verdade é que a *DarkWeb* tem menor dimensão comparativamente com a *DeepWeb.*

No entanto, na vertente da cibercriminalidade, a *DarkWeb* é utilizada, por norma, com maior frequência para a prática de ilícitos criminais que a *DeepWeb*[129]*.* Em última instância importa destacar que a *DeepWeb* e a *DarkWeb* não são utilizados, única e exclusivamente, por agentes do crime, também podem ser utilizados por sujeitos que devido à sua profissão necessitem de aceder a estes "locais" da internet, ou estão simplesmente preocupados com a sua pegada digital.

Como referido anteriormente os motores tradicionais de busca não permitem aceder às camadas mais profundas da internet. Neste sentido para que possamos aceder quer à *DeepWeb*, quer à *DarkWeb*, é preciso utilizar programas de software como, por exemplo, o *freenet* ou o *tor,* também conhecido como "*the onion routing".* Estes dois programas, especialmente, o *tor*, embora sejam utilizados maioritari- amente na *DeepWeb* a verdade é que também podem ser utilizados na *DarkWeb*. Estes programas não só permitem o acesso a estas áreas da internet como também tem potencial para impedir e prejudicar as investigações criminais em ambiente digital, embora não seja a sua principal função. Neste sentido, pretendemos distingui-los, mas também perceber o impacto que podem ter no âmbito de uma investigação criminal em ambiente digital.

Estes programas foram concebidos e desenvolvidos para salvaguardar a liberdade de expressão e informação dos seus utilizadores, todavia, têm sido aproveitados e desenvolvidos como forma de eliminar a pegada digital dos cibercriminosos.

[129] *In* SCHWALBACH, JOSÉ GASPAR. *Direito Digital.* P.29. Almedina, Coimbra, 2021.

Em relação à *freenet*[130], tem como principal objetivo evitar que utilizem a internet como um meio de monitorizar todos os seus utilizadores, algo que só será possível se eliminarmos o rasto que pode associar o autor a uma determinada informação. Esta é a única forma de exercer o direito à liberdade de expressão, totalmente livre de receios, de represálias ou censura. A principal vantagem deste programa é admitir que a informação seja depositada e esteja em constante movimento e que a sua distribuição seja o mais célere possível atendendo às necessidades dos seus utilizadores. Este formato impede que as entidades públicas conheçam a localização exata onde se encontram armazenados estes dados, e a sua origem. Estes dados são cifrados e guardados em vários dispositivos eletrónicos dos utilizadores com o intuito de dificultar o acesso aos mesmos por parte das entidades públicas.

O facto de os dados se encontrarem cifrados permite aos utilizadores negarem ter conhecimento sobre qualquer material que possa estar guardado nos seus dispositivos eletrónicos e que se reportem à *freenet*, no entanto, esta posição origina duas consequências: a primeira assenta no facto de o autor não ter controlo sobre os dados que estão guardados no seu dispositivo eletrónico e, a segunda, reside na inexistência de responsabilidade criminal para os utilizadores que tenham guardado os dados independentemente do seu conteúdo.

A *freenet* pode funcionar de dois modos distintos: *opennet* e *darknet*[131]. Aquele necessita de uma rede composta por todos os utilizadores, enquanto este apenas precisa de uma rede composta por alguns utilizadores que optem pela restrição do acesso à informação e a ficheiros partilhados num grupo restrito. O desenvolvimento deste *software* permitiu a criação de um processo mais fácil relativamente à criação, navegação e divulgação de chats, fóruns, divulgação de *websites*, bem como ao armazenamento de ficheiros e informações na *DeepWeb*.

[130] Este programa foi criado e desenvolvido por IAN CLARKE¸ no período em que frequentava a Universidade de Edimburgo no curso de inteligência artificial e ciência comportamental. Inicialmente era um novo método de navegação online que apenas podia ser executado com ajuda da instalação de um software próprio capaz de permitir ao utilizador navegar na *Web* semser detetado.

[131] *In* RAMALHO, DAVID SILVA. Investigação Criminal na Darkweb. pp. 5-7. Artigo. 2011/2012, Lisboa.

No que diz respeito ao *tor*[132], permite aos utilizadores navegar nas camadas mais profundas da *web* o que, a partida, não constitui nenhuma ilegalidade. Tornar-se-á ilegal, sim, dependendo das atividades que os utilizadores executem nessas camadas da internet. Este programa foi, inicialmente, programado para criptografar dados e enviá-los disfarçadamente em códigos aleatoriamente selecionados.

É preciso ter em atenção que cada retransmissão desencripta uma camada e assim determinar a próxima, com o intuito de passar todos os outros dados criptografados. O último código *tor* irá desencriptar uma camada mais interna e enviar dados originais para o destino final. A partir do momento em que este programa está instalado num dispositivo eletrónico, irá ocultar a sua identidade impossibilitando que terceiros possam aceder aos seus próprios trabalhos com recurso a uma rede de transmissão de dados.

Este foi o programa que teve maior impacto na evolução da cibercriminalidade, desde logo face à sua superioridade em termos de velocidade quando comparado com o outo software já desenvolvido. Com recurso a este programa foi possível desenvolver *websites* ocultos com o intuito exclusivo de cometer ilícitos cibernéticos, v.g., o *silk road*. Estes *websites* só podem ser acedidos mediante a utilização de programas de software que garantam o anonimato dos utilizadores. Ainda sobre este programa, e atendendo à EUROPOL[133], é o mais utilizado sempre que se pretende aceder da *DarkWeb*.

A utilização de criptomoedas no âmbito da navegação anónima dos utilizadores na *DarkWeb,* deve-se à impossibilidade de garantir o seu anonimato quando estavam a realizar transações online, visto que era obrigatória a intervenção de uma autoridade bancária externa à relação contratual que se estava a forma, a qual iria expor a identidade não só do comprador, como também do vendedor.

---

[132] Desenvolvido pela Marinha, no laboratório de Pesquisa Naval dos EUA, também designado por *THE ONION ROUTER*. Este programa permite aos seus utilizadores navegar na *DeepWeb* e na *DarkWeb* anonimamente, protegendo a sua identidade e privacidade enquanto navegam nas camadas mais profundas da internet.

[133] *In* IOCTA 2020: versão original. *in* EUROPOL. Internet Organised Crimes Threat Assessment. 2020.

As criptomoedas, criadas em 2009, são um meio de troca que utiliza a tecnologia *blockchain*[134], com o objetivo de validar as transações comerciais e estabelecer novas unidades de moeda.

A *bitcoin*[135], é a mais conhecida. As criptomoedas, juridicamente, foram introduzidas com outra designação, a moeda eletrónica, em 2018, segundo a diretiva da UE[136] que substituiu uma outra diretiva, igualmente da UE, a diretiva 2015/849 relativamente à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou do financiamento do terrorismo[137].

Em relação à *bitcoin*, segundo DAVID SILVA RAMALHO[138], o seu funcionamento depende de uma prévia instalação de um *software*, por parte de utilizadores com experiência e conhecimentos técnicos necessários que lhes permitam ceder parte da capacidade de processamento central ou visual dos seus dispositivos no âmbito da rede *bitcoin*. Assim sendo, cada transação efetuada é automaticamente enviada para uma rede de *peer-to-peer* para uma validação e finalmente poderá ser registada, criando um bloco de dados sobre cada uma das transações realizadas com *bitcoin*.

No que diz respeito à utilização das criptomoedas na *DarkWeb*, segundo números da EUROPOL[139], os utilizadores da *DarkWeb* não só recorrem a estas criptomoedas para comprarem tudo o que precisam, como continua a ser a escolha preferencial por eles, pese embora, o aumento que se verificou na utilização de outras modalidades de criptomoedas, v.g., *zcash* ou *monero.*

---

[134] *In* SCHWALBACH, JOSÉ GASPAR. *Direito Digital.* P.25. Almedina, Coimbra, 2021. Criado por SANTOSHI NAKAMOTO em 2008 com o propósito de servir como livro-razão no âmbito das transações de criptomoedas. Em português, literalmente, este conceito pode ser denominado de cadeia de blocos, ou seja, nome atribuído a uma lista que contem registos em crescimento e que estão ligados através da criptografia.

[135] *Idem* P.27. título de curiosidade, segundo JOSÉ GASPAR SCHWALBACH**,** a BITCOIN valia cerca de 46.031,82, uma unidade, a 27 março de 2021, e antes, a 28 de março de 2020 uma unidade valia 5.276,00. Segundo o *coinmarketcap.*com existem mais de 7.800 criptomoedas.

[136] Cf. a diretiva 2015/843 do Parlamento e do Conselho.

[137] *In* SCHWALBACH, JOSÉ GASPAR. *Direito Digital.* P.27. Almedina, Coimbra, 2021.

[138] *In* RAMALHO, DAVID SILVA. Investigação Criminal na *Darkweb*. pp. 13. Artigo. 2011/2012, Lisboa.

[139] Cf. IOCTA 2021: versão original. *In* EUROPOL. *Internet Organised Crime Threat Assessment.* 2021.

3.2. A eficácia dos Meios de Obtenção de Prova da LC e a importância da AE na *DarkWeb*

Quando nos referimos aos meios de obtenção de prova legalmente consagrados na LC o que pretendemos determinar é a sua suficiência e eficácia no âmbito de uma investigação criminal na *DarkWeb*, ou se pelo contrário deveria existir um alargamento deste núcleo. Depois de analisadas, uma a uma, iremos focar a nossa atenção na importância das ações encobertas na *DarkWeb* visto ser um dos temas fulcrais no presente estudo.

Segundo a LC, existem seis meios de obtenção de prova à disposição do investigador no âmbito de uma investigação criminal em ambiente digital, excluindo as AE[140], a saber: preservação expedida de dados informatizados[141]; a revelação expedita de dados de tráfego[142]; a injunção para apresentação ou concessão de acesso a dados[143]; a pesquisa e apreensão de dados informáticos[144]; a apreensão de correio eletrónico e registos de comunicação de natureza semelhante[145]; e, finalmente, a interceção de comunicações[146].

Posto isto, importa agora analisar cada um deles e verificar se são eficazes no combate à cibercriminalidade que ocorre na *DarkWeb*. Neste sentido a análise dos dois primeiros meios processuais será feita em simultâneo visto que a revelação expedita de dados de tráfego pressupõe a preservação expedita de dados informáticos[147], o que constituiria uma tremenda redundância visto que estaríamos a analisar duas vezes a mesma temática.

[140]Cf. análise individualizada.
[141] Consagrado no art.º 12.º da LC.
[142] Consagrado no art.º 13.º da LC.
[143]Consagrado no art.º 14.º da LC.
[144] Consagrados nos art.º 15.º e 16.º da LC.
[145] Consagrado no art.º 17.º da LC.
[146] Consagrado no art.º 18.º da LC.
[147] Nos termos da al. c) do art.º 2.º da LC: «dados de tráfego» são "os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação do destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.".

A análise destes dois meios de obtenção de prova, tem início com a revelação expedita de serviços em virtude da preservação e divulgação dos dados associados a uma determinada comunicação com a finalidade de identificar o trajeto da comunicação bem como todos os restantes elementos que sejam pertinentes, como por exemplo, a identidade dos intervenientes nessa comunicação.

No entanto, como vimos anteriormente, o programa *tor*, foi desenvolvido com o objetivo de impedir o descobrimento da identidade que se exige neste meio processual. Logo se a revelação dos dados de tráfego for autorizada antes do início da desencriptação, então será praticamente impossível aos investigadores descobrirem o destinatário daquela comunicação. Estaríamos perante uma impossibilidade técnica devido ao facto do trajeto da comunicação, que se pretende descobrir, está cifrado pelo programa *tor* impedindo descobrir a verdade.

No que diz respeito à injunção para apresentação, ou concessão do acesso de dados, pode ser executada de duas formas. A primeira através da apresentação da injunção ao fornecedor de serviço. A segunda, terá de ser apresentada ao administrador da rede informática utilizada pelo agente quando acede à *DarkWeb*. Em relação à primeira forma, é fundamental abrir duas hipóteses[148]. A primeira hipótese, assenta na obtenção de dados específicos que estão armazenados num determinado sistema informático. Atendendo a esta situação a questão, reside no facto do fornecedor de serviços estar num *website* que só pode ser acedido através da *DarkWeb*. Ainda sobre esta hipótese é fundamental determinar a localização exata do sistema informático, algo que poderá ser praticamente, impossível a não ser que tenham sido adotadas medidas de segurança que o permitam.

A injunção só funciona se os dados forem transmitidos diretamente ao fornecedor de serviço, o que não acontece. Logo podemos concluir que esta injunção não irá produzir os efeitos que se pretende no âmbito de uma investigação criminal na *DarkWeb*.

[148] Cf. o n.º 1 do art.º 14.º da LC e também, segundo a al. a) a c) do n.º 4 do art.º 14.º da LC.

Na segunda hipótese, refere-se à obrigação exigida pelo fornecedor de serviços na revelação dos dados, com base no disposto nas als. a) a c) do n.º 4 do art.º 14.º da LC, o que significa que o fornecedor de serviços tem um cliente que através desta ligação consegue navegar na *DarkWeb*. Em relação a esta hipótese, a conclusão será semelhante, ou seja, a injunção não produzirá os efeitos que se pretende, visto que o fornecedor de serviço teria de ter a capacidade para detetar o sistema informático de onde surgiu a comunicação que avisa o acesso à *DarkWeb*. Esta possibilidade seria praticamente impossível se estivermos perante um utilizador cuidadoso e com os conhecimentos informáticos necessários para evitar essa situação. No que concerne à segunda forma[149], a única possibilidade de produzir efeitos no seio da investigação criminal será se o agente do crime não tiver tido cuidado na utilização das medidas anti forenses no seu sistema informático, por exemplo, se por qualquer motivo não cifrou os dados antes de transmiti-los, ou ainda, se o motor de busca que utilizou não estava configurado para armazenar toda a informação dos sites visitados[150].

Neste sentido, poderemos concluir que a utilização deste meio de obtenção de prova no âmbito de uma investigação criminal na *DarkWeb* será infrutífera, visto que, regra geral, os agentes do crime não são descuidados a este ponto quando navegam na *DarkWeb,* ou até mesmo na *DeepWeb.*

Em relação aos outros meios processuais em análise importa ainda destacar, a apreensão de dados informáticos, atendendo a uma tripla distinção que é necessário realizar, visto que a apreensão de dados pode ocorrer em três momentos completamente distintos, nomeadamente, através de uma pesquisa num sistema informático[151], ou uma extensão dessa mesma pesquisa, mas noutro sistema informático[152] acedido com base na pesquisa inicial; e, por último, um outro acesso legitimo a um sistema informático especifico[153].

[149] Importa referir que as anteriores hipóteses levantadas se reportavam à primeira forma.
[150] Quer através do cache, quer através das *cookies*.
[151] Nos termos do n.º 1 do art.º 15.º da LC.
[152] Nos termos do n.º 5 do art.º 15.º da LC.
[153] Nos termos do n.º 1 do art.º 16.º da LC.

No entanto, para que exista uma efetiva apreensão dos dados é fundamental determinar, não só, o sistema informático onde se encontram armazenados, como também se podemos aceder aos mesmos e, em caso afirmativo e, se sim, a partir de que sistema foi possível, independentemente da modalidade utilizada. Só conseguiríamos chegar a uma conclusão se o investigador estivesse numa posição que lhe permitisse ter acesso ao dispositivo eletrónico do agente do crime, ou então, de algum modo infiltra-se na *DarkWeb*. Assim sendo, para resolver esta questão teriam de ser executadas outras atividades de extrema importância.

A este respeito existe uma outra questão, que poderá ou não emergir, antes da própria apreensão de dados, e que assenta na obtenção de credenciais, por parte do investigador, v.g., nomes de utilizador, palavras-passe, que lhe permitem ter acesso aos sites que se encontram localizados na *DarkWeb*.

A partir do momento em que estes problemas estão solucionados dá-se início à apreensão de dados informáticos. A apreensão de dados informáticos começa com a própria confiscação do computador ou de outro dispositivo eletrónico que foi utilizado para aceder à *DarkWeb*. Em relação aos dados que se visa apreender, são essencialmente todos aqueles que permitam estabelecer uma conexão entre o utilizador do dispositivo eletrónico apreendido e a atividade ilícita que foi cometida. No que diz respeito a este meio, a recolha de prova na *DarkWeb* exige que se respeitem as regras forenses no âmbito digital para que se possa fazer uma validação dos dados informáticos e, também determinar a exata localização física do sistema informático onde se encontram armazenados os dados para recolha.
A localização destes dados[154], é de extrema importância porque não só permite realizar a pesquisa que levará à apreensão destes dados, mas também é importante para a autorização da extensão desta pesquisa noutro sistema informático,

[154] Com fundamento no n.º 1 do art.º 15.º da LC.

que não o primeiro, e onde possam estar localizados os dados[155] que se pretende recolher. Estes requisitos têm de ser respeitados para que a recolha de prova possa ser validade no âmbito da ciência forense digital.

Em suma, podemos afirmar que este meio de obtenção de prova é promissor no âmbito da investigação criminal na *DarkWeb* mas sempre no pressuposto do investigador, ser alguém, com conhecimentos prévios no que concerne ao *website* utilizado pelos criminosos. Este é o meio de obtenção de prova que, no âmbito desta matéria, deve merecer maior destaque no futuro porque pode trazer contributos fundamentais para a investigação criminal. Relativamente à apreensão de correio eletrónico e o registo de comunicações de natureza semelhante, não exige uma análise do mesmo modo que os anteriores meios de obtenção de prova. É suficiente afirmar, que no âmbito da *DarkWeb* e com tudo o que já vimos sobre esta realidade, estamos perante um meio sem relevo neste âmbito. O mesmo se aplica ao último meio de obtenção de prova, que falta analisar, que se reporta à interceção de comunicações[156].

Em relação às AE em ambiente digital o seu fundamento assenta na LC[157], mais concretamente no art.º 19.º deste diploma. Este meio processual, em comparação com os outros já analisados, é bem mais agressivo para os direitos fundamentais, logo merece um tratamento melhor do que lhe foi dado na LC. De todos os meios já analisados, este é sem dúvida aquele que proporciona mais vantagens numa investigação criminal na *DarkWeb,* exemplo disto, é o caso dos EUA, onde se tem verificado resultados muito positivos mediante a utilização das AE em ambiente digital, especialmente em crimes, v.g., combate ao jogo ilegal, tráfico de droga, pornografia e pedofilia online. Este impacto que se tem verificado nos EUA é o mesmo que pretendemos que ocorra em Portugal, no nosso ordenamento jurídico.

[155] Nos termos do n.º 5 do art.º 15.º da LC.
[156] Com base no disposto no n.º 4 do art.º 18.º da LC.
[157] Neste contexto foi possível suprir uma lacuna que existia no nosso direito processual penal, pois até então não existia a referência das AE em ambiente digital, apenas em ambiente físico regulado no CPP. No entanto não está devidamente detalhado, ou seja, em virtude da sua danosidade é fundamental que o seu regime jurídico esteja o mais detalhado possível.

A agressividade é uma das suas características que permite levar a bom porto uma investigação criminal na *DarkWeb,* como sucedeu num caso particular nos EUA[158]. Este é um caso que demonstra bem a importância que as AE em ambiente digital acarretam no seio da investigação criminal pois não só permite um processo de integração do agente da polícia numa determinada comunidade digital em virtude de um descuido do criminoso que permite às autoridades judiciárias não só identificá-los como também recolher todos os ficheiros num determinado dispositivo eletrónico e que tenham valor probatório.

O principal problema que se poderá apontar a este meio processual é a sua incapacidade para produzir resultados positivos quando esteja em causa o acesso a *websites* que não permitam interação entre os seus membros, e outros que só permitem a introdução de imagens ou vídeos ilícitos com o objetivo de partilhá-los com outros membros para que estes possam não só visualizá-los como também fazer *download* dos mesmos. Para estas situações era fundamental que estivesse consagrado no nosso ordenamento jurídico a possibilidade de se utilizar o *Malware* como meio de obtenção de prova, visto que através dele não será obrigatório estabelecer relações de confiança com os suspeitos de ilícitos criminosos.

4. Inovação à atual Lei do Cibercrime

Como já verificamos anteriormente, a LC não é totalmente aceite no nosso ordenamento pela doutrina, ou seja, existem autores que elaboram várias críticas a esta lei, principalmente pela forma como foram concebidos os seus preceitos legais e alguns destes autores questionam a sua própria constitucionalidade. Como vimos esta lei não é pacifica. Nós não só concordamos com algumas das críticas, já analisadas, como também fazemos uma critica à LC, e que assenta no facto de não

[158] Este caso ficou conhecido como o "Monstro de Riga". Neste caso um agente do FBI, na qualidade de agente encoberto, persuadiu um individuo assíduo em chats e fóruns dedicados à pedofilia online, remete-lhe uma fotografia onde constava um homem adulto a abusar sexualmente de uma criança de apenas 18 meses. Com base nesta foto enviada ao individuo e através de uma análise visual da mesma permitiu um enorme desenvolvimento no caso, transpondo a investigação criminal diretamente para outro país. Já nesse país, segundo divulgação de imagens da menor, foi possível identificar o seu agressor. Mais tarde veio a verificar-se que o perpetrador deste crime era também assíduo destes websites na *DarkWeb*, o que levou a polícia holandesa a infiltrasse em alguns desses chats para recolher o material necessário.

prever o *Malware* como um meio oculto de obtenção de prova. Para que esta seja uma nova realidade no nosso ordenamento jurídico é imprescindível uma regulamentação densa e concreta, como se verifica com outros meios ocultos de obtenção de prova, pelo que nunca poderemos subsumir a sua aplicação nos dias de hoje, como alguns autores proferem.

Neste sentido, não concordamos com alguns autores que afirmam que podemos subsumir a sua aplicação, atualmente, por força de algumas disposições na LC. Deste modo, o que propomos é uma solução inovadora, à atual LC, o que consideramos ser benéfico e uma mais-valia para o nosso ordenamento jurídico, mas principalmente, no âmbito da investigação criminal em ambiente digital, mais concretamente na *DarkWeb*.

O que nós propomos é a elaboração de um novo diploma legal ou uma simples alteração legislativa à LC, onde preveja não só a consagração legal do *Malware* como um meio oculto de obtenção de prova, mas também toda a extensão do seu regime jurídico, não deixando nada por escrever. Esta novidade no nosso ordenamento jurídico implica conhecimentos técnicos especializados ao legislador, os quais devem ser adquiridos anteriormente a esta atualização, ou então, a atualização terá de ser feita em parceria com um técnico especializado, nesta área, que possa esclarecer qualquer conceito ou dúvida que o legislador tenha durante o período em que está a desenvolver a nova lei.

Caso contrário poderia ser criada uma lei que não tem aplicação prática ou o seu conteúdo será insuficiente quando aplicada ao caso concreto, como sucede com outras leis.

4.1. Solução Apresentada

Antes de passarmos à explanação da nossa posição relativamente a esta matéria e da proposta que apresentamos é necessário fazermos um enquadramento prévio sobre se de facto o nosso ordenamento jurídico permite a introdução do *Malware* no leque dos meios ocultos de obtenção de prova já consagrados em legislação avulsa, como acontece com o RJAE e a LC, as legislações mais em foque no presente estudo. Para esta análise, socorremo-nos da conjugação dos arts.º 125.º e 126.º do CPP, visto que esta temática se centra no âmbito do DPP. Neste sentido, é no âmbito do art.º 125.º do CPP que se encontra estabelecido o princípio da legalidade de prova, o que significa que são admitidas todas provas que não sejam proibidas por lei.

Assim sendo, podemos afirmar, inequivocamente, que o sistema de prova, estabelecido no nosso ordenamento jurídico, é um sistema de prova livre, ou de liberdade de prova, como queiramos, pelo que não é exigido que um meio de obtenção de prova esteja expressamente consagrado na lei para que possa ser utilizado. Esta é a regra geral do nosso sistema de prova em Portugal.

Todavia estamos no âmbito dos meios ocultos de obtenção de prova, os quais se encontram sujeitos a restrições de duas ordens, quer no plano constitucional, quer no plano legal. Os primeiros, tal como o nome indica, decorrem da CRP, mais concretamente da aplicação do n.º 8 do art.º 32.º da CRP[159]. Por outro lado, as restrições legais surgem por aplicação do art.º 126.º do CPP, onde se estabelece, no n.º 1 e n.º 2, as provas que são consideradas absolutamente proibidas[160], aquelas que nunca podem ser utilizadas pois afetam direitos que a CRP considera serem invioláveis, como por exemplo, o art.º 25.º da CRP[161].

---

[159] Nos termos do qual se estabelece que "(…) 8. são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, domicílio, na correspondência ou nas telecomunicações. (…)".

[160] *In* CPP, ou seja, este art.º prevê que "(…) 1. São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas. (…)". O n.º 2 do mesmo preceito legal concretiza, a fundo, as ofensas da integridade física ou moral das pessoas.

[161] Segundo o qual, "1. A integridade moral e física das pessoas é inviolável.
2. Ninguém pode ser submetido a tortura, nem a tratos ou penas cruéis, degradantes ou desumanos.".

Além da referência às provas absolutamente proibidas, o art.º 126.º do CPP, consagra as provas que são relativamente proibidas[162] e que se reportam a direitos que a própria CRP considera que podem ser limitados em situações expressamente consagradas neste diploma, nomeadamente o art.º 26.º[163] e o n.º 3 e 4 do art.º 34.º[164].

A possibilidade de se admitir provas relativamente proibidas traduz-se da própria CRP, no n.º 8 do art.º 32.º, como já mencionado, visto que só serão nulas as provas que sejam recolhidas mediante "intromissão na vida privada, domicílio, na correspondência ou nas telecomunicações", ou seja, em situações sem intervenção judiciária e que se verifiquem fora dos casos consagrados na lei, ou ainda, quando não se cumpra o princípio da proporcionalidade, nos termos e para efeitos, do n.º 2 do art.º 18.º da CRP. *A contrario*, será admitida "intromissão na vida privada, domicílio, na correspondência ou nas telecomunicações" desde que seja um caso previsto na lei, ou que tenha prévia autorização judiciária, e sempre que respeite o pressuposto no n.º 2 do art.º 18.º da CRP, ou seja, que se cumpra o princípio da proporcionalidade.

Tendo em atenção o panorama que existe atualmente no nosso ordenamento jurídico no que respeita a esta matéria, achamos por bem dar o nosso contributo, expondo não só a nossa posição sobre a matéria aqui em análise, como também o que consideramos que deve ser feito neste contexto, para que no futuro possamos resolver qualquer caso que aconteça, independentemente da sua complexidade.

---

[162] Atendendo ao disposto neste preceito estão "(…) 3 – ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular. (…)".

[163] Cf. "1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação. (…)".

[164] Segundo o qual, "(…) 3. Ninguém pode entrar durante a noite no domicílio de qualquer pessoa sem o seu consentimento, salvo em situação de flagrante delito ou mediante autorização judicial em casos de criminalidade especialmente violenta ou altamente organizada, incluindo o terrorismo e o tráfico de pessoas, de armas e de estupefacientes, nos termos previstos na lei.

4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal.".

Neste sentido, reconhecemos a necessidade de se enquadrar o *Malware* como um meio oculto de obtenção de prova pois não existe nenhum outro como ele na panóplia de meios de obtenção de prova no âmbito da nossa legislação, sendo a ação encoberta aquele que mais se aproxima. Estamos cientes da sua "danosidade social"[165]. A potencial lesão dos direitos constitucionais e, ou, processuais, obriga a uma previsão legal deste instrumento com maior clareza, densidade e precisão, evitando ambiguidades na interpretação de conceitos. A atual LC é incapaz de dar resposta. A realidade é que estamos na presença de um instrumento indispensável na prevenção e investigação criminal perante novas formas de criminalidade contemporânea, e a sua utilização pode nos trazer enormes vantagens, no futuro.

Segundo COSTA ANDRADE, a criminalidade altamente organizada, o terrorismo, o terrorismo internacional, entre outros, em virtude das suas caraterísticas, nos dias de hoje, são o equivalente a um santuário que não é afetado pela devassa dos meios tradicionais e "abertos" de investigação que as autoridades competentes tem a sua disposição, sendo fundamental e imprescindível criar novos meios de obtenção de prova com especificidades distintas, tal com o *Malware* apresenta, pese embora viole algumas garantias processuais do arguido. Todavia, em nome da descoberta da verdade material e respetiva boa condução do processo e da investigação criminal, consideramos imperioso que a sua eventual aplicação no caso concreto venha suprimir com as necessárias limitações todos os direitos constitucionais e processuais, consoante o caso concreto. No entanto, o princípio da descoberta da verdade não pode estar acima de todos os DLG consagrados na CRP, e por isso mesmo foram estabelecidos limites, para proteger os direitos fundamentais consagrados na CRP.

[165] Visto que não só afeta vários direitos constitucionais como também direitos processuais, nomeadamente, direitos do arguido. No entanto consideramos que no caso concreto, tudo ponderado,assente nos princípios da necessidade e da proporcionalidade aqueles devem ser suprimidos afavor da descoberta da verdade material, outro princípio constitucional para o sucesso da investigação criminal realizada nesse âmbito. Caso contrário seria impossível solucionar, ou prevenir, essa situação, dependendo se estivéssemos no âmbito da prevenção ou da investigação criminal.

A restrição aos direitos fundamentais só poderá ser realizada depois de uma interpretação constitucional, será válida sempre que se demonstre que é justificada e adequada na prossecução dos objetivos da investigação criminal. No fundo, a restrição dos direitos fundamentais terá sempre de ser enquadrada no âmbito do princípio da proporcionalidade, da necessidade e da adequação. O nosso entendimento é de que, atualmente, não existe nenhuma norma habilitante que preveja a utilização do *Malware* como meio de obtenção de prova e é inadiável a criação dessa norma no âmbito da LC. No entanto, essa norma terá de ser desenvolvida com uma técnica legislativa, nos limites da perfeição, sem deixar nada por escrever, desenvolver mais extensamente, possível, o seu regime jurídico para que não haja várias interpretações sobre os conceitos e evitar a discricionariedade das ações, respeitando todos os princípios. Como é evidente, este instrumento não pode ser aplicado em qualquer situação e de qualquer modo, pelo que a sua aplicação tem de estar sujeita a várias restrições, limitações.

Neste sentido é importante identificar e analisar os princípios que devem ser cumpridos quando esta norma entrar em vigor, tornando-a infalível. Em primeiro lugar, o princípio da reserva de lei, o que significa que a aplicação deste instrumento jamais poderá ser feita através de submissões a regime jurídico alheio, ou seja, é impossível utilizarmos o *Malware* como meio de obtenção de prova por aplicação de um regime jurídico que diga respeito a um outro meio de obtenção de prova, por mais verosímil que possa ser. A aplicação do *Malware* como meio oculto de obtenção de prova terá que obrigatoriamente estar consagrado em legislação no nosso ordenamento jurídico, caso contrário nunca será permitida durante uma investigação criminal. Este princípio torna-se mais importante quando estamos perante os meios ocultos de obtenção de prova dada a sua implicação nos direitos fundamentais e nos princípios e direitos processuais. A aplicação de *Malware* terá de estar, obrigatoriamente, vinculada a este princípio, porque em primeira instância tem de ser elaborada uma nova lei, ou uma alteração à atual LC, a contemplar tal possibilidade.

Segundo COSTA ANDRADE[166] as leis já existentes não podem ser analisadas como normas penais em branco, o que é proibido no âmbito do direito penal, ou seja, não podem ter uma amplitude que permita adotar "novos meios técnicos de invasão e devassa".

Outro princípio que deve ser respeitado é o princípio da proporcionalidade, i.e., para que se possa aplicar este instrumento, como meio de obtenção de prova, terão de existir limitações, melhor dizendo, supressões não só das garantias processuais, v.g., do arguido, mas também dos seus direitos fundamentais com o objetivo de se atingir o bom andamento da investigação criminal e, em última instância, a descoberta da verdade material. No entanto é preciso ter noção que esta supressão nunca será total, nem poderá ser realizada de qualquer modo, visto que terá sempre de se ter em conta a proporcionalidade entre o que se pretende descobrir com a utilização deste instrumento e os direitos, ou garantias, que se pretende suprimir. É no âmbito deste princípio que consideramos imprescindível o estabelecimento de um catálogo de crimes, quando se estiver a desenvolver o seu regime jurídico. Este catálogo, irá contemplar uma lista taxativa de crimes sobre os quais se poderá, única e exclusivamente, aplicar o *Malware* como meio de obtenção de prova.

No fundo, este instrumento não poderá ser aplicado em qualquer situação que ocorra, face à sua "danosidade". Neste sentido só poderá ser aplicado em situações de especial complexidade, v.g., criminalidade organizada, terrorismo, cibercriminalidade, pedofilia online. A eventual utilização do *Malware*, no nosso ordenamento jurídico, terá de respeitar o princípio da adequação ou idoneidade. Neste caso, o que está em causa, é a relação entre o meio empregue no caso concreto e o que se pretende obter com a utilização do mesmo. A aplicação do *Malware* num determinado caso só poderá suceder se aquele for adequado, emvirtude das necessidades naquele momento.

[166] *In* 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.* P. 113, Coimbra Editora, 2009.

O princípio da necessidade ou exigibilidade e subjacente a este o princípio da subsidiariedade são também muito importantes nesta matéria e que devem ser igualmente respeitados. Assim sendo, é preciso compreender, no caso concreto, se este novo meio é o único que pode alcançar os resultados que se pretendem, isto é, se é necessário para o efeito. É neste contexto que surge, então, o princípio da subsidiariedade, que nos obriga a analisar o caso concreto e perceber se não existe ou não, no âmbito dos meios de obtenção de prova que temos à nossa disposição, quer sejam "abertos", ou obscuros, um outro meio de obtenção de prova menos gravoso que aquele e consiga atingir os mesmos resultados. Se a conclusão for afirmativa, e existir de facto um outro meio de obtenção de prova menos gravoso que a utilização de *Malware*, no caso concreto, então teremos de optar pelo meio menos gravoso, e nunca, pelo *Malware*. Em sentido inverso, se a conclusão for negativa, e não existir um meio de obtenção de prova menos gravoso que o *Malware* para solucionar a questão, então teremos de utilizar este novo instrumento, uma mais-valia não só para combater as medidas anti-forenses, mas também no combate à criminalidade organizada e, sobretudo,contra a cibercriminalidade.

Existem ainda outros princípios importantes e que merecem destaque, nomeadamente, o princípio da proporcionalidade em *stricto sensu* e, o princípio da reserva do juiz. No que diz respeito, ao primeiro, a questão reside na relação entre o que se pretende obter em particular com a utilização deste instrumento e as restrições dos direitos no caso concreto, e que servirá sempre para inviabilizar a adoção de meios restritivos, desproporcionais e excessivos em virtude dos objetivos que se pretende atingir.

Em relação ao princípio da reserva do juiz, é importante que fique discriminado a competência, i.e., terá de ficar expresso no seu regime jurídico qual a entidade competente para permitir a sua utilização no caso concreto. No nosso entendimento deverá constar na norma habilitante que a admissibilidade, ou não, de se utilizar o *Malware* como meio de obtenção de prova deverá recair sobre o JIC que detem, exclusivamente, o poder de tomar tal decisão. Além de ser fundamental respeitar todos estes princípios, consideramos que é importante destacar outros critérios que devem ser levados em consideração no momento da elaboração desta

nova lei, ou da alteração à atual LC, nomeadamente, um critério temporal, um critério pessoal e um critério procedimental, ou seja, é necessário que se inclua não só, o período em que este meio deve ser utilizado, o modo como deve ser instalado e o como funcionará. Além do mais, terá de indicar o visado.

Neste sentido, importa escrutinar todas as exigências que consideramos que devem ser cumpridas quando se estiver a elaborar o regime jurídico do *Malware*, enquanto meio oculto de obtenção de prova. A primeira exigência que deve constar neste novo regime jurídico, será a mesma que consta do título dado à lei n.º 101/2001 de 25 agosto[167], ou seja, o *Malware* enquanto meio oculto de obtenção de prova também deverá ser aplicado, não só no âmbito da investigação criminal, mas também na prevenção criminal, evitando a ocorrência de danos gravosos para a sociedade. Deve estar sujeito, igualmente, a uma exigência legal, no sentido em que a sua utilização, como meio oculto de obtenção de prova, só será admitida mediante requerimento apresentado pelo MP ao JIC e, depois deste, autorizar o mesmo.

Em relação ao regime jurídico que deve existir tem de respeitar os seguintes critérios: critério temporal, i.e., a legislação que vier a consagrar a utilização do *Malware* terá que, obrigatoriamente impor um período de curta duração para que o AE possa utilizá-lo no âmbito da investigação, ou prevenção, criminal em ambiente digital, mais concretamente na *DarkWeb.* Este período terá de ser, v.g., ou de três meses renovável por período igual, ou então, por seis meses renovável por um período nunca superior a três meses. Por outras palavras, a utilização deste instrumento nunca poderá exceder um ano de utilização, porque seria uma violação grosseira do n.º 2 do art.º 34.º da CRP, mas também não poderá ser inferior a seis meses, porque limitaria a atuação do AE, no sentido em que este precisa de tempo não só para instalar o *Malware* no dispositivo eletrónico, ou sistema informático do(s) suspeito(s) e, em seguida, estabelecer relação com o(s) mesmo(s). Em suma, a utilização inferior a um período de seis meses será muito curta, mas superior a um ano será demasiado.

[167] RJAE: regime jurídico das ações encobertas para fins de prevenção e investigação criminal

Outro critério que deve ser cumprido é o critério pessoal no sentido em que este instrumento só poderá ser aplicado contra o(s) suspeito(s) do crime que se pretende investigar, ou prevenir. Assim sendo, toda e qualquer informação relevante que for obtida através de outro individuo não poderá ser recolhida e, por conseguinte, ser utilizada no processo. Não pode ser instalado no dispositivo eletrónico, ou no sistema informático de alguém, que não o(s) suspeito(s), caso isso aconteça a informação deve ser destruída ou simplesmente não ser junta aos autos.

Finalmente, o último critério fundamental que deve ser tido em linha de conta, é o critério procedimental, ou seja, o funcionamento do *Malware* e a sua instalação não devem ficar ao livre-arbítrio do AE. Deve ficar consagrado, no seu regime jurídico, o modo como este instrumento deve ser instalado no dispositivo eletrónico, ou sistema informático, poderá ser instalado física ou remotamente, e ambas as opções devem constar depois ficará a cabo do AE, consoante o caso em concreto, optar pela mais vantajosa, todavia consideramos que a via mais utilizada deve ser a instalação remota, pois garante uma maior proteção para o AE e a sua família, diminuindo, consideravelmente, o risco de ser descoberto.

Outra questão muito importante, e que deve ser tida em consideração durante todo este processo, é a de saber se a utilização do *Malware* engloba todas as suas modalidades, elencadas anteriormente, ou só devem ser admitidas algumas, ou em última instância, apenas uma das modalidades analisadas.

Importa não esquecer, que nos EUA e na Alemanha, não são admitidas todas as modalidades, inclusive já existiram recusa de algumas modalidades, como foi devidamente destacado anteriormente. No que diz respeito ao seu âmbito de aplicação, algo que ainda não foi abordado, consideramos que este instrumento deve estar sujeito a um catálogo taxativo de crimes, o que significa que só poderá ser aplicado a crimes de especial gravidade, e a cibercrimes, ou seja, o catálogo de crimes a que este meio está sujeito deverá ser o mesmo, ou idêntico, ao constante do art.º 19.º da LC, relativamente ao regime jurídico das AE em ambiente digital, facilitando deste modo a compatibilização destas duas realidades no âmbito da prevenção , investigação criminal na *DARKWEB.*

Estes são, fundamentalmente, os critérios e as exigências, que o regime jurídico do *Malware* deve cumprir para que não fiquem dúvidas sobre a sua utilização e quando devem utilizar. Todas estas referências devem constar expressamente.

4.2. Compatibilidade entre *Malware* e AE

Procuramos analisar se existem ou não condições, ou se podem ser criadas, para que o *Malware* possa ser utilizado pelo agente encoberto no âmbito de uma investigação criminal na *DarkWeb.* Para que tal suceda é necessário averiguar se existem semelhanças entre estas duas realidades e se, do ponto vista jurídico, podem ser compatíveis. Desde logo, e atendendo ao supramencionado, com fundamento na conjugação dos arts.º 125.º e 126.º do CPP, nada impede o *Malware* de ser introduzido no leque dos meios ocultos de obtenção de prova onde se insere, naturalmente, as AE. Este leque engloba não só as ações encobertas, como também, videovigilância, localização celular, buscas online, escutas telefónicas e ainda, a interceção de correspondência eletrónica[168]. Eventualmente, esperemos nós, irá consagrar também o *Malware*.

Segundo COSTA ANDRADE[169], existem duas características comuns a todos estes meios ocultos de obtenção de prova, a saber: "o carater institucionalizado das medidas de ingerência, patente na legitimação material e formal-procedimental que a própria ordem jurídica confere e o carater de generalização das mesmas medidas".

[168] *In* NEVES, RITA CASTANHEIRA. *As ingerências nas comunicações eletrónicas em processo penal: Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova. p. 96.* Coimbra Editora, 2011.
[169] *Idem.* p. 101.

Este carater oculto é fundamental para o sucesso da investigação criminal, porque se os suspeitos soubessem previamente que o OPC, iria utilizar qualquer um destes meios para recolher provas contra si e da prática do crime, nunca iriam se comprometer ao ponto de utilizar dispositivos eletrónicos que permitissem a recolha de prova, porque se o fizessem estariam deliberada e conscientemente a proporcionar provas contra si, as quais poderiam ser utilizadas durante um processo crime.

O combate à criminalidade mais grave, nomeadamente, cibercriminalidade, terrorismo, criminalidade organizada, não pode ser feito do mesmo modo que se combate as outras formas de criminalidade menos gravosas. Não podemos utilizar os mesmos métodos de obtenção de prova, porque o *modus operandi* dos criminosos esta em constante desenvolvimento, e portanto também os meios de recolha de prova ao serviço do OPC deve acompanhar essa evolução.

Assim sendo, o facto de estes meios de obtenção de prova poderem ser utiliza-dos contra os suspeitos sem que estes tenham conhecimento, ou consentido, na sua utilização, exigem uma atualização de princípios[170] consagrados no nosso ordenamento jurídico e que que devem ser respeitados por todos, mas principal-mente, pelos meios ocultos de obtenção de prova visto que que estes meios são os mais intrusos nos direitos das pessoas e, por isso, mesmo só podem ser aplicados em situações muito excecionais. Até contra o criminoso mais asqueroso se deve colocar limites à investigação com o objetivo de garantir que a sua dignidade humana não seja afetada pela intervenção das autoridades.

Os princípios a que nos referimos, e que já foram analisados anteriormente, são: o princípio da reserva de lei; princípio da proporcionalidade, o princípio da adequação, o princípio da necessidade; o princípio da subsidiariedade e, ainda, o princípio da reserva de lei. É importante que a consagração de um meio, oculto,

[170] *Idem.* p.97.

de obtenção de prova na lei preveja com antecedência uma medida que constrinja o direito que se pretende comprimir[171] e, caso isso não aconteça, ou essa previsão não seja suficiente então a utilização desse meio de obtenção de prova será proibido, sendo impossível o recurso à analogia.

Os meios ocultos de obtenção de prova, violam não só direitos fundamentais, como também direitos e princípios processuais. Nos primeiros englobamos: o direito à privacidade; o direito à palavra, direito à inviolabilidade das comunicações privadas, e do domicílio. Em relação aos segundos podemos encontrar, v.g., o direito ao silêncio do arguido, direito a recusar testemunho ou depoimento, o princípio *nemo tenetur se ipsum acusare*, o princípio do julgamento justo e equitativo e permitem, ainda, obter "confissões inconscientes" por parte dos suspeitos, que desconhecem que estão a ser vigiados pelo OPC[172].

Deste modo, iremos analisar os vários direitos em questão, percebendo o seu conteúdo e o modo como são violados pela utilização destes meios ocultos de obtenção de prova, e ao mesmo tempo, compreender até que ponto podem ou não ser limitados no âmbito de uma investigação criminal para que se possa recorrer ao *Malware* ou às AE, ou ainda, a ambos.

O direito à privacidade, nos termos do art.º 26.º da CRP vem, inclusivamente, regulado no CPC, segundo entendimento da doutrina[173], este direito engloba três esferas distintas e as quais merecem destaque individualmente, visto que nem todas podem ser restringidas a favor da descoberta da verdade material. As três esferas dividem-se, na: esfera íntima; esfera privada e, esfera pessoal. A primeira é completamente inviolável, é impossível restringi-la onde encontramos os sentimentos, emoções, questões sobre sexualidade e, portanto, não se pode intervir seja de que modo for. É demasiado pessoal, e por isso nenhuma autoridade ou outros particulares pode invadir.

[171] *In* NEVES, RITA CASTANHEIRA. *As ingerências nas comunicações eletrónicas em processo penal: Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova.* p.99. Coimbra Editora, 2011.
[172] Idem. pp.100-101.
[173] *Ibidem.* p.37. Influenciada, de certo modo, pelo ordenamento jurídico alemão.

A segunda esfera, reporta-se ao próprio individuo relativamente ao seu passado, à sua história e ao contexto social em que foi inserido. No âmbito da esfera da privacidade[174], importa referir, que é possível que seja restringida, em processo penal, se encontrar em conflito com a utilização de um meio oculto de obtenção de prova, mas sempre nos limites da ponderação, segundo o art.º 18.º da CRP. A última esfera não deixa de ser associada ao individuo, mas já não é tao intimista como as anteriores, incide mais sobre a sua vida pública, não só profissionalmente, mas também as suas relações na comunidade em que está inserido. Assim sendo, tudo o que diga respeito a esta esfera da intimidade, pode estar sujeita a restrições atendendo a uma prévia ponderação dos interesses envolvidos. Em consonância, COSTA ANDRADE[175], vem nos dizer que a esfera mais restritiva de todas, ou seja, a espera da intimidade, e como tal, só diz respeito a aspetos associados à sexualidade, saúde, entre outros, mas que existe claramente um confronto entre os outros dois domínios de cada pessoa.

Neste contexto encontramos o parecer do Conselho Consultivo da Procuradoria-Geral da República n.º 16/94[176], que veio defender a diferenciação do direito à privacidade em três esferas: a esfera íntima, esfera privada e a esfera pública.

[174] *In* NEVES, RITA CASTANHEIRA. *As ingerências nas comunicações eletrónicas em processo penal: Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova.* p.40. Coimbra Editora, 2011.
[175] *Idem. p.42.*
[176] *Ibidem.* p.41 “vida íntima (que abrange os “gestos e factos relativos ao estado do sujeito enquanto separado do grupo e a certas relações sociais que devem em absoluto ser subtraídos ao conhecimento de outrem”) vida privada (que abrange os “acontecimentos partilhados com um nº restrito de pessoas”) e vida pública (que abrange os “eventos respeitantes à participação de cada um na vida da coletividade e por isso suscetíveis de ser conhecidos por todos”)”.

Outro direito que será violado com a utilização do *Malware* e as AE, é o direito à palavra, tal como o direito á intimidade, não é estanque, tem duas dimensões[177]que tem de ser analisadas em separado: a dimensão da palavra falada, e a dimensão da palavra escrita. Em relação à primeira dimensão, esta goza de uma proteção constitucional mais intensa em virtude do seu cariz volátil e pelo facto de que será impossível reproduzir exatamente essas palavras num outro contexto, seja ele qual for. Este bem jurídico protege não só a inviolabilidade das comunicações, como também a privacidade dos indivíduos. No que concerne à outra dimensão, a palavra escrita, a realidade já não é a mesma porque a partir do momento em que estas palavras são proferidas ficam redigidas, quer seja no ambiente físico, ou, no mundo digital, irão permanecer para sempre e, portanto, podem facilmente ser replicadas noutro contexto. A palavra escrita não goza da mesma proteção constitucional que é atribuída à palavra falada, visto que já cumpriu o seu principal objetivo que é a comunicação, logo é possível que exista uma limitação à mesma. Em sentido contrário é absolutamente proibido restringir o direito à palavra falada.

Importa realçar que a principal razão para que estas duas dimensões não tenham a mesma proteção constitucional, deve-se ao facto, de que na palavra escrita a probabilidade de errar ou comprometer o seu significado alterando o contexto em que é utilizado é mínimo, e por tanto no âmbito do DP, não se justifica uma igual proteção. A este respeito, quem nos esclarece melhor é JOSÉ DE FARIA COSTA[178], segundo o qual "é obvio que por outro lado, para nós, o falar é muito mais do que aquilo que se diz em texto. Correndo o risco da distorção conceitual (…) poder-se-á afirmar que a palavra é o suposto, a condição e, simultaneamente, o "essencial" segmento (…) do humano. Somos, porque somos seres falados. E porque seres falados somos seres pensados".

[177] *Idem.* p.46.
[178] *Ibidem.* p.46

O mesmo autor, dá-nos conta de uma nova palavra, a palavra virtual, atendendo ao desenvolvimento tecnológico dos últimos anos. No entanto somos da opinião que não deve existir uma terceira dimensão porque esta novidade pode-se subsumir a ambas as dimensões já analisadas. Por exemplo, se estivermos a comunicar via *skype*, ou *zoom*, essa palavra virtual é ao mesmo tempo uma palavra falada. E, ao contrário, se estivermos a utilizar o correio eletrónico, ou o *whatsapp*, para comunicar, então a palavra virtual é, em simultâneo, uma palavra escrita.

O direito à inviolabilidade das comunicações ou da correspondência, consagrado no n.º 1 do art.º 34.º da CRP, é provavelmente o direito fundamental mais fustigado com a utilização das AE, o que se irá agudizar ainda mais com a consagração do *Malware* no nosso ordenamento jurídico como novo meio oculto de obtenção de prova. Este direito o que nos vem dizer é que qualquer sujeito deve-se sentir seguro, quando pretende comunicar com outrem, seja por que meio for, v.g., correio eletrónico ou a correspondência tradicional, de que ninguém irá ter acesso ao seu conteúdo e divulgar o mesmo, quer seja mediante a interceção ou a gravação das referidas comunicações. Esta segurança deve ser proporcionada pelo Estado.

Pese embora, a CRP nos diga que as comunicações são invioláveis sendo proibida qualquer ingerência nas mesmas, a verdade é que é admissível a intervenção de autoridades nestas comunicações, mas em casos excecionais, ou seja, a CRP no n.º 4 do art.º 34.º[179], admite a possibilidade de as autoridades poderem ter acesso às comunicações dos cidadãos, mas apena se só em casos que estejam previamente consagrados no processo penal, caso contrário será impensável essa ingerência. É com fundamento nesta exceção constitucional que foram desenvolvidos no âmbito do DPP, meios ocultos de obtenção de prova, v.g., apreensões eletrónicas e escutas telefónicas.

[179] Cf. n.º 4 do art.º 34.º CRP: "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo penal" *in* ::: Decreto de 10 de Abril de 1976 (pgdlisboa.pt)

Nesta lógica, será com fundamento nesta exceção que se irá permitir a utilização do *Malware* no leque de meios de obtenção de prova porque não só permite ter acesso às comunicações efetuadas, como também, nos permite visualizá-las e ouvi-las em tempo real.

Esta possibilidade consagrada na CRP, não se aplica exclusivamente às formas de criminalidade mais gravosas, como é o caso, da cibercriminalidade, da criminalidade organizada, ou do terrorismo, como também se aplica a todos os crimes que constem, v.g., catálogo de crimes consagrado no regime jurídico das escutastelefónicas.

Outro direito que pode ser confrontado com a utilização destes instrumentos, é a autodeterminação informacional, regulada no art.º 35.º da CRP, porque a utilização de *Malware* pode indicar-nos o perfil do utilizador em questão, atendendo à quantidade e qualidade da informação que possa ser recolhida do sistema informático. Este direito resulta do desenvolvimento de um outro direito já analisado, mas no contexto das novas tecnologias de informação, o direito à privacidade. Este direito reconhece ao individuo o direito de conhecer e dar consentimento ao tratamento dos seus dados pessoais, protegendo-o em momentos "contra a recolha, armazenamento, uso e transmissão ilimitados de dados pessoais[180]. Todavia estas proteções conferidas aos cidadãos podem sofrer limitações quando em causa estejam interesses gerais da comunidade, mas sempre com fundamento constitucional.

Depois de analisados os DLG que podem ser violados, iremos a analisar no âmbito do DPP, os princípios e direitos processuais associados ao arguido e que são violados com a utilização dos meios ocultos de obtenção de prova, começando pelo princípio da audiência e defesa, previsto no n.º 1 e 2 do art.º 32.º da CRP, segundo o qual, deve se dar a possibilidade ao arguido de ser ouvido antes que se tome qualquer decisão que afete os seus direitos, ou seja, deve poder examinar as provas que são apresentadas pela acusação, ou seja, este direito

[180] *In* BATISTA, JORGE LYDIE. *O Malware como Meio de Obtenção de Prova em Processo Penal.* p.73. Dissertação de Mestrado, 2018

não podia ser mais contrário à utilização do *Malware* como meio oculto de obtenção de prova, porque o fundamento para a sua utilização, e o sucesso da mesma, assenta no desconhecimento, e falta de consentimento, por parte do arguido da instalação deste instrumento nos seus dispositivos eletrónicos, ou sistema informático apenas tendo conhecimento da instalação, durante o processo quando a prova fosse apresentada.

Seria impensável, numa situação prática, comunicarmos ao arguido que o JIC tinha autorizado a instalação de *Malware* no seu dispositivo eletrónico, porque isso inviabilizaria automaticamente a finalidade deste instrumento. A partir daquele momento, o arguido nunca mais iria utilizar aquele dispositivo eletrónico, ou pelo menos, durante o período em que o *Malware* estivesse instalado, porque sabia que toda a sua atividade ficaria registada e poderia ser utilizada pelo OPC em sede de julgamento, inclusive as suas comunicações. Mesmo que durante o julgamento tomassem conhecimento da utilização deste instrumento dificilmente conseguiria opor-se, porque a invasão à sua vida já ocorreu, e de certo modo, com a sua atividade, ainda que de forma inconsciente, contribuíram para a acusação que lhes foi feita. Em suma, este é um princípio que claramente seria violado com a utilização do *Malware* como meio oculto de obtenção de prova, e o mesmo se aplicará na utilização das AE.

Outro princípio que claramente é violado com a utilização destes instrumentos como meios de obtenção de prova, é o princípio do contraditório[181], ou seja, a possibilidade que o arguido tem de realizar contraprova, em igualdade de forças, face à prova recolhida e apresentada pela acusação. E o fundamento para a sua violação será essencialmente o mesmo que justifica a violação do princípio anteriormente analisado, porque o desconhecimento por parte do arguido de que o *Malware* foi utilizado para recolha de prova "impossibilita-o" de contestar a validade da prova apresentada, e a fonte de onde foi extraída, porque até aquele momento desconhecia o modo como a prova tinha sido recolhida.

[181] Consagrado no n.º 5 do art.º 32.º da CRP.

Este é um princípio que, na nossa opinião, iria ser suprimido, ou, restringido nestas situações porque seria muito difícil, para o arguido conseguir apresentar factos que contrariassem a informação recolhida pelo *Malware*, ou até, suficiente para criar dúvida no juiz de julgamento. É óbvio que o *Malware* não é 100% eficaz, aliás como nenhum outro meio de obtenção de prova é, mas a sua margem de erro será muito diminuta. Portanto torna-se difícil, talvez mesmo "impossível", o arguido conseguir apresentar factos que contrariem a prova obtida através deste novo meio de obtenção de prova, até mesmo o suficiente para gerar a dúvida no juiz de julgamento. É neste sentido que afirmamos que este princípio será violado, ou em certa medida, restringido.

Ainda a este respeito, o princípio *Nemo Tenetur Se Ipsum Accusare* é outro que será violado com a introdução desta nova realidade. Segundo este princípio[182], o arguido não é obrigado a autoincriminar-se, tanto não é, que em audiência de julgamento quando é chamado para responder às questões, o Mm.º juiz de direito, adverte-o que na qualidade de arguido não é obrigado a responder às questões que lhe forem colocadas, e o facto de não responder não o prejudica. O direito a não se autoincriminar não se reporta, única e exclusivamente, ao direito ao silêncio, já mencionado, mas também na vertente de não ter de apre- sentar meios de prova.

Neste sentido, torna-se claro, que este princípio pode ser violado, porque como já referido anteriormente, a utilização de *Malware*, ou até mesmo das AE, exige o desconhecimento, e falta de consentimento do arguido para a utilização destes instrumentos, e caso soubessem perderiam a sua eficácia, logo, o facto de não saberem faz com que durante o período em que estes instrumentos estão implementados, o(s) arguido(s) irá agir normalmente, comunicando com outros, como se nada estivesse acontecer, e inconscientemente está a autoincriminar-se por- que está a facultar ao OPC, provas que poderão ser utilizadas contra si, em sede de julgamento, e que de outra forma, provavelmente, nunca teriam sido descobertas se o arguido soubesse que, efetivamente, naquele período de tempo estava a ser vigiado mediante a utilização de *Malware*.

[182] Cf. base legal nos seguintes arts.º do CPP: al.d) do n.º 1 do art.º 61.º; al. a) do n.º 4 do art.º 141.º; n.º 1 do art.º 343.º e, o n.º1 do art.º 345.º.

É neste contexto que compreendemos a real utilidade e os benefícios que este instrumento poderia proporcionar na atividade do OPC, no âmbito da investigação criminal. Também o princípio do *in dúbio pro reo*[183] ou da presunção de inocência, pode ser violado, ou pelo menos, a sua eficácia prática pode ser inútil com a possível utilização do *Malware* como meio de obtenção de prova na investigação criminal. Este princípio permite, em caso de dúvida, perante a prova produzida, o Mm.º Juiz decidir a favor do réu[184], mas na eventualidade da utilização do *Malware* a dúvida deixará de existir porque, partindo do pressuposto, que sejam cumpridos todos os requisitos exigidos e consagrados na futura lei, para a utilização deste instrumento não haverá qualquer dúvida da parte do Mm.º Juiz da culpabilidade do arguido no cometido do ilícito criminal ou, da verificação do ilícito criminal, pois o *Malware* permite a recolha de prova, em tempo real, e sem o consentimento do arguido o que proporciona um "contributo", da parte deste, mesmo desconhecendo que está a facilitar a recolha de prova.

Nem se coloca a situação de "casos em que, muito embora a prova produzida contenha probabilidades muito elevadas a favor da hipótese da acusação, no entanto, por si só, essas probabilidades não excluem, ou não podem excluir, a dúvida suscitada nas hipóteses alternativas de facto"[185], porque a utilização do *Malware* permite uma certeza absoluta, não há muito espaço para erro, a menos, claro que o AE tenha de algum modo criado, provocado, a prova que está a recolher e, nesse caso, como vimos, será nula, não poderá ser valorada em sede de audiência de julgamento. A prova recolhida e, consequente, ação do AE deve ser analisada escrupulosamente.

183 Cf. o AC. TRL, processo n.º 518/08.7PLLSB.L1-5, de 14-10-2010, " o principio "*in dúbio pro reo"* não é mais que uma regra de decisão: produzida a prova e efetuada a sua valoração, quando o resultado do processo probatório seja uma dúvida razoável e insuperável sobre a realidade dos factos, ou seja, subsistindo no espirito do julgador uma dúvida positiva e invencível sobre a verificação, ou não, de determinado facto, o juiz deve decidir a favor do arguido, dando como não provado o facto que lhe é desfavorável. (…) só vale para dúvidas insanáveis sobre a verificação ou não de factos (objetivos ou subjetivos) relevantes, quer para a determinação da responsabilidade do arguido, quer para a graduação da sua culpa". *In* Acórdão do Tribunal da Relação de Lisboa (dgsi.pt)

184 Segundo o Ac. TRL., processo n.º 433/15.8PBSNT.L1-9, de 28-09-2017, " (…) todos os factos relevantes para na decisão desfavoráveis ao arguido que, face à prova não possam ser subtraídos à dúvida razoável do julgador não podem dar-se como provados (…)" *in* Acórdão do Tribunal da Relação de Lisboa (dgsi.pt)

185 Segundo Ac. TRP., processo n.º 17583/18.1T9PRT.P1, de 10-05-2023. *In* Acórdão do Tribunal da Relação do Porto (dgsi.pt)

Finalmente, em relação aos direitos processuais, existem autores que afirmam que o direito de recusar o testemunho será violado com a utilização destes instrumentos. Nós não conseguimos compreender como isso seria possível de acontecer visto que este é um direito que assiste ao arguido, seja em que situação for ele nunca é obrigado a prestar declarações e o facto de se poder utilizar o *Malware*, ou as AE, numa investigação criminal contra si, para facilitar a recolha de prova não irá prejudicar em nada o seu direito. Independentemente do meio de obtenção de prova que seja empregue, nenhum deles irá obrigá-lo a prestar declarações porque é seu direito, enquanto arguido num processo-crime, não prestar declarações em sede de audiência de julgamento. Neste sentido, temos dificuldade em compreender como a utilização de um meio oculto de obtenção de prova iria colocar em causa o seu direito de recusar a depor. Por mais evidente que seja a prova recolhida e que ele desconheça que foi a utilização do Malware que esteve na origem daquela recolha nada o impedirá, no momento oportuno, manifestar a sua intenção perante o Mmº Juiz a sua intenção de não prestar depoimento, primeiro porque é um direito seu, e segundo porque o facto de não prestar declarações não o vai desfavorecer em nada.

Conclusão

Como se pode constatar, o presente estudo, assenta fundamentalmente na análise de duas realidades distintas, mas que se podiam complementar no âmbito de uma investigação criminal levada a cabo na *DarkWeb*, tanto é assim que a pergunta de investigação central incide sobre a compatibilidade entre estes dois instrumentos numa investigação criminal em ambiente digital. Todas as outras questões que foram formuladas, às quais também pretendemos responder, serviam de base para fundamentarmos devidamente a nossa posição relativamente à questão central. Por isso mesmo, iremos responder a todas as questões que suscitamos numa fase embrionária, que abordam o *Malware* e as AE, individualmente, porque assim irá permitir uma resposta devidamente fundamentada à pergunta de investigação central.

Assim sendo, atualmente, no ordenamento jurídico português, não se contempla a consagração do *Malware* como meio oculto de obtenção de prova, no CPP, nem mesmo na LC, onde deveria estar regulada, e muito menos na restante legislação avulsa. Pese embora, a Convenção que fundamenta a implementação da LC no nosso ordenamento jurídico, ou seja, a Convenção do Cibercrime, consagre claramente a utilização deste instrumento no leque dos meios de obtenção de prova, no combate à cibercriminalidade, mediante a utilização da expressão, "em tempo real", repetidamente nos arts.º 20.º e 21.º, da referida Convenção[186].

Se consultarmos a atual LC, desde o art.º 11.º ao 19.º, referentes aos meios de obtenção de prova verificamos que nem por uma vez, o legislador utilizou esta expressão, sendo fácil a compreensão que atualmente não é possível aplicar o *Malware* no âmbito de uma investigação criminal na *DarkWeb*, por falta de consagração legal e, consequente, violação do princípio da reserva de lei.

[186] *In* 0635406378.pdf (dre.pt). p.19. A "recolha em tempo real, de dados de tráfego (…) em tempo real, dos dados de conteúdo de comunicações especificas feitas no seu território, transmitidas através de um sistema informático".

Tal como nos diz, RITA CASTANHEIRA NEVES, não esta previsto no nosso ordenamento tal possibilidade e, como tal, não se deve subsumir a aplicação desta realidade a nenhum art.º da LC. No mesmo sentido, existem outros autores como, PAULO DÁ MESQUITA, que é da mesma opinião, ou seja, não se deve misturar as duas realidades, visto que em nenhum dos arts.º consagrados na LC é possível englobar a instalação e a utilização deste instrumento. A este respeito, também JULIANA CAMPOS[187], é da opinião que não pode ser enquadrado, nem ao abrigo da LC, nem de nenhuma outra norma legal que diga respeito aos meios de obtenção de prova no ordenamento jurídico português.

No entanto, apesar de nos depararmos perante uma realidade em que não existe norma habilitante, isso não significa que será sempre assim, mesmo porque vimos que nós temos um sistema de prova livre, nos termos e para efeitos do art.º 125.º do CPP, e que a utilização de um meio de obtenção de prova não necessita a sua regulação expressa, mas como estamos perante a criação de um meio oculto de obtenção de prova com consequências graves para vários direitos constitucionais e garantias processuais, como vimos, é necessário que a utilização de novos meios ocultos de obtenção de prova se encontrem regulados tal como sucede, por exemplo, com as AE "tradicionais" e as AE em ambiente digital.

A futura utilização deste instrumento recairia necessariamente no âmbito do n.º 3 do art.º 126.º do CPP, *"ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular*.", ou seja, seria recairia no âmbito das provas relativamente proibidas. Atualmente, e enquanto não existem avanços nesta matéria, vários autores da nossa doutrina, afirmam que é possível subsumir a aplicação do Malware com base no leque de meios de obtenção de prova consagrados na LC.

[187] *In* CAMPOS, JULIANA FILIPA SOUSA. *O uso de Malware como meio de obtenção de provaem processo penal.* p.103. Almedina, Lisboa, 2021.

Desde logo, DAVID SILVA RAMALHO, autor com várias obras neste âmbito, pese embora, reconheça que o *Malware* deva ter um regime jurídico mais denso e devidamente detalhado considera que atualmente já é possível aplicar este instrumento no âmbito dos meios ocultos de obtenção de prova que já estão consagrados no nosso ordenamento jurídico através da sua subsunção ao n.º 2 do art.º 19.º da LC porque o legislador quando utilizou a expressão "sendo necessário o recurso a meios e dispositivos informáticos" não se estava a referir aos meios já consagrados na LC mas aqueles que não estão consagrados como tal, nomeadamente, o *Malware*. Ao mesmo tempo, explica o porquê de não se puder subsumir noutras disposições legais da LC, nomeadamente o n.º 1 e n.º 5 do art.º 15.º e o n.º 2 do art.18.º.

Em sentido contrário PAULO PINTO DE ALBUQUERQUE considera que devemos subsumir a aplicação do *Malware* ao art.º 15.º da LC, com fundamento na expressão "pesquisa em sistema informático", mas claramente estaríamos a limitar o âmbito de aplicação do *Malware*, visto que esta realidade permite muito mais do que uma mera pesquisa em sistemas informáticos. No entanto, afirma que se assim fosse, seria inconstitucional por violação do n.º 1 e n.º 2 do art.º 26.º e do n.º 4 do art.º 34.º da CRP, por considerar que é uma clara violação da intromissão na privacidade do sujeito visado e totalmente desproporcional.

Nós somos da opinião de que efetivamente não existe previsão legal que autorize a aplicação do *Malware* como meio oculto de obtenção de prova, expressa ou através de subsunção. Em relação à subsunção, a existir seria apenas nos termos estipulados por DAVID SILVA RAMALHO, porque nos parece ser a fundamentação mais coerente. Todas as outras posições que envolvem o art.º 15.º ou o art.º 18.º, definitivamente que não tem em consideração o conceito de *Malware*, definido como sendo um programa de *software* que é instalado secretamente num determinado sistema informático, sem o consentimento do visado, com o intuito de expor dados confidenciais e a integridade dos mesmos[188].

[188] *In* MONTEIRO, ERICK WALLACE CARNEIRO CALAÇA DIAS. *Ações Encobertas no Mundo Virtual: a problemática da tutela da privacidade como barreira à obtenção de provas nas redes sociais.* P.15. Dissertação de mestrado científico em Ciências Jurídico-Criminais. Lisboa, 2018.

Independentemente das várias modalidades, qualquer uma possibilita, em conjunto, as seguintes atividades[189]: vigilância em tempo real, cópia dos dados armazenados no sistema, e ainda, é possível ativar remotamente a câmara e microfone dos dispositivos eletrónicos. Ou seja, através do *Malware*, podemos fazer, não só, o que nos é permitido com os outros meios de obtenção de prova já existentes na LC, mas também executar outras tarefas que seriam impensáveis de executar com os meios de obtenção de prova consagrados naquele diploma aplicáveis à investigação criminal em ambiente digital, mas especificamente no combate à criminalidade que se verifica na *DarkWeb*. Neste sentido, o conceito de *Malware* subsumido a qualquer preceito normativo consagrado na LC estaríamos a limitar o seu próprio conceito como também a sua própria área de atuação.

No que diz respeito ao regime jurídico consagrado no RJAE, face às ações encobertas em ambiente físico, e o regime jurídico consagrado no art.º 19.º da LC, relativamente às ações encobertas em ambiente digital, constatamos que apesar de serem duas realidades completamente distintas a verdade é que ambos os regimes jurídicos, com exceção do catálogo de crimes que é distinto em ambos, são iguais, por força da aplicação do n.º 1 do art.º 19.º da LC, segundo o qual "é admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de agosto".

Apesar de compreendermos a opção tomada pelo legislador em 2009, data em que entrou em vigor a LC, a verdade é que atualmente não se justifica esta previsão legal e, exige-se que se promova a uma alteração legislativa no seio do regime jurídico da AE em ambiente digital, visto se tratar de uma realidade muito mais vasta e com incontáveis formas dos criminosos praticarem crimes neste meio, e o atual regime não permite ao OPC uma investigação justa e compatível com a realidade que tem de enfrentar.

[189] *Idem.*

Atualmente o regime jurídico das AE em ambiente digital é insuficiente perante a panóplia de crimes que os criminosos conseguem executar em ambiente digital, principalmente na *DarkWeb*, dificultando atuação do OPC. Como referimos anteriormente, são duas modalidades de AE, mas são realidades distintas especialmente do ponto de vista operacional. Desde logo, o AE tem a oportunidade de criar múltiplas identidades fictícias e utilizá-las ao mesmo tempo em diferentes sítios da internet, ao passo que no ambiente físico, o AE é obrigado a estar presencialmente num determinado local a observar o que está a acontecer, e como tal não se pode "desdobrar" em várias pessoas para vigiar diferentes locais ao mesmo tempo. Além do mais, pode desenvolver várias identidades, nenhuma que se assemelhe a sua, naturalmente, e em simultâneo estar em conversações com diferentes suspeitos de diferentes crimes em diferentes fóruns chats, entre outros, inclusive pode utilizar vários perfis na mesma conversação com o suspeito da prática do crime.

Tudo isto a partir do conforto do seu gabinete, v.g., correndo muito menos riscos que em ambiente físico. Neste contexto surge a outra diferença, visto que em ambiente digital os riscos que o AE corre são muito menores quando comparados com aqueles a que esta sujeito o AE em ambiente físico, pois não tem de mostrar o seu rosto, a sua aparência porque através de um computador pode estar em qualquer zona territorial, salvaguardando a sua segurança, imagem e evitando futuras represálias contra si, ou contra a sua família pelos criminosos que investiga. A sua atuação, no ambiente digital, é muito mais veloz porque lhe permite conversar com vários suspeitos num único momento, interagindo com os mesmos independentemente do local em que se encontrem, visto que não se tem de deslocar até eles e estabelecer um contacto direto, presencial. Além do mais possui várias ferramentas que o podem auxiliar na sua atuação e que dificilmente conseguiria utilizar nas AE em ambiente físico. Todas estas diferenças reforçam a ideia de que deve existir uma alteração legislativa densificando o regime jurídico das AE em ambiente digital.

Relativamente à questão central deste estudo, atendendo ao que foi dito e a tudo o que foi analisado para efeitos de recolha de informação, podemos concluir que efetivamente estas duas realidades, o *Malware* e o agente encoberto, podem ser compatibilizadas no âmbito de uma investigação criminal, do ponto de vista teórico.

Desde logo, pelo sistema de prova livre assente no DPP, por força do art.º 125.º, que não exclui absolutamente a utilização de *Malware* como meio oculto de obtenção de prova no futuro. Este instrumento terá sempre de ser desenvolvido no âmbito dos meios ocultos de obtenção de prova, caso contrário perderia a sua eficácia e operacionalidade pois a sua utilização parte do pressuposto que o visado desconhece a sua utilização. A partir do momento em que tenha esse conhecimento será muito mais cuidadoso nas suas movimentações na internet, tornando inoperável este instrumento. Em seguida, o facto de ambos serem meios ocultos de obtenção de prova, o que significa que podem ser utilizados sem o conhecimento, ou consentimento do visado e apenas podem ser utilizados contra crimes de cibercriminalidade ou criminalidade de elevada danosidade, v.g., terrorismo, tráfico de pessoas e menores, criminalidade organizada, quer seja no âmbito da prevenção ou da investigação como resulta do título da lei n.º 101/2001 de 25 de agosto.

O *Malware* será sempre um meio mais intrusivo que as próprias ações encobertas, por isso mesmo só poderá ser aplicada em situações muito excecionais, como as já elencadas, e a sua utilização deverá sempre respeitar os princípios da proporcionalidade, necessidade e adequação, assentes no princípio da subsidiariedade. Importa destacar que os mesmos princípios devem reger todos os meios ocultos de obtenção de prova e por conseguinte deverá ser aplicado ao *Malware* e à AE em ambiente digital. Além do mais, a utilização destes meios de obtenção de prova pode conflituar com um vasto leque de DLG consagrados na CRP e a sua restrição dependerá deste mesmo diploma. São afetados direitos, como o direito à reserva da intimidade, o direito à palavra, o direito à imagem, o direito à inviolabilidade do domicílio, direito ao segredo das comunicações, direito à autodeterminação informacional, direito à integridade e confidencialidade dos sistemas informáticos.

Não só coloca em risco estes direitos fundamentais, como viola vários princípios processuais atinentes ao processo penal, nomeadamente, princípio da audiência e defesa, princípio do contraditório, princípio do julgamento justo e equitativo, direito a recusar testemunho ou depoimento.

Bibliografia

ANDRADE, MANUEL DA COSTA. *"Bruscamente no verão passado", a reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente.* Coimbra Editora, 2009.

BATISTA, JORGE LYDIE. *O Malware como Meio de Obtenção de Prova em Processo Penal.* Dissertação de Mestrado, 2018.
Disponível em: Repositório da Universidade de Lisboa: O malware como meiode obtenção de prova em processo penal (ul.pt)

CAMPOS, JULIANA FILIPA SOUSA. *O Malware como Meio de Obtenção da Prova em Processo Penal. A Investigação Oculta em Ambiente Digital.* Coimbra, Almedina, 2021.

CARVALHO, CAIO. TOR: Conheça o Programa Anti-Espionagem que deixa você anónimo na internet. CANALTECH, 2013.
Disponível em: Tor: conheça o programa anti-espionagem que deixa você anônimo na internet - Canaltech

CATANA, ANTÓNIO JOSÉ DA SILVA. *A Natureza Jurídica da Ação do Agente Infiltrado Digital.* Dissertação de Mestrado em Ciências Policiais, especialização em Criminologia e Investigação Criminal. Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI). Lisboa, 2018.

GOMES, DANIEL JOSÉ AFONSO. *O controlo da Ação do Agente Encoberto à luz do ordenamento jurídico português.* Dissertação de Mestrado em Direito e Prática Jurídica, especialidade de Direito Penal. Universidade de Lisboa, Facul- dade de Direito. Lisboa, junho de 2019.

GUEDES, ANA RITA ALMEIDA. *O Agente Encoberto Digital enquanto Método Oculto de Obtenção de Prova.* Dissertação no âmbito do 2º ciclo de Estudos em Ciências Jurídico-Forenses. Universidade de Coimbra. Coimbra, outubro de 2021.

LIMA, ADELINA. Surface web e deep web: qual a diferença entre elas?. Artigo publicado em 2021.
Disponível em: Surface web, deep web e dark web: qual é a diferença? (r7.com)

LIMA, ANA CATARINA RATO. *A figura do Agente Provocador e consequências da sua atuação em matéria de prova.* Mestrado em Direito e Prática Jurídica com especialidade em Ciências Jurídico-Forenses. Lisboa, 2020.

MANN, DIANA CALAZANS. *Infiltração Digital: A validade como meio de prova e os limites éticos do Estado-Investigador.* Dissertação do VII Mestrado não integrado em Ciências Policias no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI), especialização em Criminologia e Investigação Criminal.

MESQUITA, PAULO DÁ. *Processo Penal, Prova e Sistema Judiciário.* Coimbra Editora, outubro 2010.

MONTEIRO, ERICK WALLACE CARNEIRO CALAÇA DIAS. *Ações Encobertas no Mundo Virtual: a problemática da tutela da privacidade como barreira à obtenção de provas nas redes sociais.* Dissertação de mestrado científico em Ciências Jurídico-Criminais. Lisboa, 2018.

NEVES, RITA CASTANHEIRA. *As ingerências nas comunicações eletrónicas em processo penal: Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova.* Coimbra Editora, 2011.

OLIVEIRA, JOÃO COSME TEIXEIRA DE. *Investigação no crime organizado: métodos ocultos de investigação a partir da atuação do agente infiltrado.* Dissertação de Mestrado. Universidade Lusíada. Porto. 2015.

RAMALHO, DAVID SILVA (org.). *Coletânea de Legislação sobre Cibercrime e Prova Digital*. Lisboa, AAFDL Editora, 2021

RAMALHO, DAVID SILVA. *A investigação Criminal na DarkWeb.* Relatório de Mestrado em Ciências Jurídico-Criminais. Faculdade de Direito da Universidade de Lisboa. 2011/2012.
Disponível em: CR14_15_-_David_Silva_Ramalho.pdf (concorrencia.pt)

RAMALHO, DAVID SILVA. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra, Almedina, 2017 reimpressão 2019.

RAMALHO, DAVID SILVA. *O uso de Malware como Meio de Obtenção de Prova em Processo Penal.* Art.º de 2013.
Disponível em: O uso de malware como meio de obtenção de prova em processo penal, Livros e Artigos Científicos, Conhecimento - Sérvulo & Associados - Sociedade de Advogados, Portugal (servulo.com)

RAMOS, ARMANDO DIAS. *O Agente Encoberto Digital. Meios Especiais e Técnicos de Investigação Criminal.* Coimbra, Almedina, 2022.

RAMOS, ARMANDO REIS DIAS. *O Agente Infiltrado Digital: Contributo para o estudo das vicissitudes da recolha de prova em direito penal informático.* Tese Doutoramento em Direito, especialidade em Ciências Jurídicas. Lisboa, 2017

REGO, SARA DANIELA QUINTAS COUTO. *Do Agente Encoberto ao Agente Provocador.* Dissertação de Mestrado em Direito Criminal, Universidade Católica Portuguesa. Porto, maio 2016.

RIBEIRO, MARA LEONORA ANTUNES. *O espaço de atuação do Agente Encoberto Digital: entre a Lei das Ações Encobertas e o Art. 19º da Lei do Cibercrime.* Dissertação no âmbito do 2º ciclo de Estudos em Ciências Jurídico-Criminais. Universidade de Coimbra. Coimbra, maio de 2022.

RIBOLI, EDUARDO BOLSONI. *A utilização de novas tecnologias no âmbito da investigação criminal e as suas limitações legais: a interceptação de comunicações em massa e os softwares de espionagem.* Revista de Direito e Economia, volume XIX, 1 julho a 31 dezembro, 2018. Lisboa.

RODRIGUES, BENJAMIM SILVA. *Da prova penal. tomo II Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*. P. 37. 1ªedição, Editora Rei dos Livros, Lisboa, 2010.

SALES, BEATRIZ. O que é a Deep Web e como entrar?. Artigo publicado em 2017. *Disponível em*: O que é a Deep Web e como entrar? - Segredos do Mundo (r7.com)

SALUTES, BRUNO. O que é o Cache? Saiba apagá-lo no celular e no computa-dor. CANALTECH, 2019.
Disponível em: O que é cache? - Canaltech

SCHWALBACH, JOSÉ GASPAR. *Direito Digital*. Coimbra, Almedina, 2021.

SILVA, ANDRÉ TIAGO RIBEIRO. *As Ações Encobertas à Luz do Processo Penal Português*. Dissertação de Mestrado em Direito e Prática Jurídica, especialidade em Ciências Jurídico-Forenses. FDUL, 2019.

SILVEIRA, MARIA ANA BARROSO DE MOURA DA. *Da problemática da investigação criminal em ambiente digital – em especial sobre a possibilidade da utilização de Malware como Meio Oculto de Obtenção de Prova*. Tese de Mestrado na Universidade Católica Portuguesa, 28 de março de 2016. *Disponível em:* Tese final 28 Março.pdf (ucp.pt)

TEIXEIRA, DANIEL ALEXANDRE BARBOSA. *Ações Encobertas: Limites Constitucionais*. Dissertação de Mestrado. Faculdade de Direito, Universidade Nova de Lisboa. Lisboa, setembro 2018.

Links consultados:

BELCIC, IVAN. *O que é malware e como se proteger contra-ataques de malware.* Artigo publicado a 20 janeiro de 2023.
Disponível em: O que é malware e como funciona | Definição de malware | Avast

BURDOVA, CARLY. *O que é um rootkit e como removê-lo?.* Artigo publicado a22 de julho de 2021.
Disponível em: O que é rootkit e como removê-lo? | Avast

CARVALHO, CAIO. *TOR: conheça o programa anti-espionagem que deixa você anônimo na internet.* Artigo publicado a 9 de outubro de 2013.
Disponível em: Tor: conheça o programa anti-espionagem que deixa você anô-nimo na internet - Canaltech

ESET. *Guia de Ransomware.*
Disponível em: 2021-ESET-guia-ransomware-PT.pdf

ESET. *O que é um cavalo de troia?.*
Disponível em: O que é um malware Cavalo de Tróia - como remover e perma-necer protegido | ESET

ESET. *O que é Spyware?*.
Disponível em: O que é spyware? | ESET

EUROPOL. Internet Organised Crime Threat Assessment. 2021.
Disponível em: Internet Organised Crime Threat Assessment (IOCTA) 2021 | Eu-ropol (europa.eu)

EUROPOL. Internet Organised Crimes Threat Assessment. 2020.
Disponível em: Internet Organised Crime Threat Assessment (IOCTA) 2020 | Europol (europa.eu)

FURQUIM, THIAGO. *O que é cache?*. Artigo publicado a 2 de março de 2023.
Disponível em: O que é cache? - Canaltech

GHIMIRAY, DEEPAN. *O que é uma bomba lógica? Como impedir ataques de bomba lógica.* Artigo publicado a 22 abril de 2021.
Disponível em: O que é bomba lógica? Examplos e prevenção | Avast

GUGELMIN, FELIPE. *Entenda o que é backdoor e a diferença com os trojans*. Artigo publicado a 4 de agosto de 2021.
Disponível em: Entenda o que é backdoor e a diferença com os trojans - Canal-tech

KOVACS, LEANDRO. *O que é engenharia social?*. Artigo publicado em 2021 e atualizado em 2023.
Disponível em: O que é Engenharia Social? – Tecnoblog

KOVACS, LEANDRO. *O que é backdoor em computação?*. Artigo publicado a2021, atualizado em 2023.
Disponível em: O que é backdoor em computação? – Tecnoblog

LATTO, NICA. *Worm X Vírus: descubra as diferenças e os perigos dessas ameaças.* Artigo publicado a 13 de agosto de 2020.
Disponível em: Vírus X Worm de computador: Qual é a diferença? | Avast

LATTO, NICA. *O que é e como funciona um vírus de computador.* Artigo publicado a 12 de fevereiro de 2020.
Disponível em: O que é vírus de computador? | Definição de vírus de PC | Avast

LATTO, NICA. *O que são keyloggers e como funcionam?.* Artigo publicado a 11 agosto de 2019.
Disponível em: O que é um keylogger? Definição de registro de digitação | Avast

LIMA, ADELINA. *Surface web, deep web e dark web: qual é a diferença?.* Artigode 17 de novembro de 2021, atualizado a 11 de fevereiro de 2022.
Disponível em: Surface web, deep web e dark web: qual é a diferença? (r7.com)

MINISTÉRIO PÚBLICO. *Cibercrime em 2020 – Denúncias Recebidas.* 12 janeirode 2021.
Disponível em: Cibercrime em 2020 – denúncias recebidas | GabinetedeCiber-crime (ministeriopublico.pt)

MINISTÉRIO PÚBLICO. *Cibercrime em 2021 (1º Semestre) – Denúncias Recebidas*. 23 julho de 2021.
Disponível em: Cibercrime em 2021 (1º Semestre) – denúncias recebidas | GabinetedeCibercrime (ministeriopublico.pt)

MINISTÉRIO PÚBLICO. *Convenção sobre o Cibercrime.* Consulta de Tratados Internacionais.
Disponível em: Convenção sobre o Cibercrime | Portal do Ministério Público - Portugal (ministeriopublico.pt)

REGAN, JOSEPH e BELCIC, IVAN. *O que é malware? O guia definitivo para o Malware.* Artigo de 14 de fevereiro de 2022.
Disponível em: O que é malware? | O que faz e como funciona | AVG

SEGUIN, PATRICK e LATTO, NICA. *Guia Básico sobre Ransomware.* Artigo publicado a 24 de setembro de 2021.
Disponível em: O que é ransomware e como se proteger | Avast

SALES, BEATRIZ. *O que é a Deep Web e como entrar?* Artigo publicado a 5 de dezembro de 2017 e, atualizado a 29 de outubro de 2021.
Disponível em: O que é a Deep Web e como entrar? - Segredos do Mundo (r7.com)

SANTOS, LEVI ALVES DOS. *Os ataques Ransomware e a camada de proteção em sistemas governamentais.* Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano, 2007, Ed.08, vol.04, pp. 132-161. Agosto de 2022.

Disponível em: Os ataques ransomware e a camada de proteção em sistemas (nucleodoconhecimento.com.br)

SEGUIN, PATRICK. *Spyware: Deteção, Prevenção e Remoção.* Artigo publicadoa 20 de fevereiro de 2020.
Disponível em: O que é spyware? | Definição de spyware | Avast

SPINATO, TIAGO PROTTI. *Ransomware e Cibersegurança: a informação ameaçada por ataques a dados.* Dissertação de Mestrado na Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI). 25 de maio de 2020, Rio Grande do Sul.
Disponível em: Vista do Ransomware e cibersegurança: a informação ameaçada por ataques a dados (uninove.br)

Legislação Consultada:

Lei do Cibercrime
RJAE
Código Processual Penal
Constituição da República Portuguesa
Convenção sobre o Cibercrime