Universidade do Minho
Escola de Direito

Ana Teresa Seabra de Oliveira

Obtenção de Prova Digital: Utilização de *Malware* pelos Órgãos da Polícia Criminal

outubro de 2017

Ana Teresa Seabra de Oliveira **Obtenção de Prova Digital: Utilização de *Malware* pelos Órgãos da Polícia Criminal**

UMinho|2017

Universidade do Minho
Escola de Direito

Ana Teresa Seabra de Oliveira

Obtenção de Prova Digital: Utilização de *Malware* pelos Órgãos da Polícia Criminal

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação do
Professor Doutor Pedro Miguel Fernandes Freitas
e do
Professor Doutor Vítor Francisco Mendes Freitas Gomes Fonte

outubro de 2017

DECLARAÇÃO

Nome: Ana Teresa Seabra de Oliveira

Endereço eletrónico: ana.seabra.oliveira@hotmail.com

Número do Cartão de Cidadão: 13753160 5 ZY0

Título dissertação: Obtenção de Prova Digital: Utilização de *Malware* pelos Órgãos da Polícia Criminal

Orientadores:

Professor Doutor Pedro Miguel Fernandes Freitas

Professor Doutor Vítor Francisco Mendes Freitas Gomes Fonte

Ano de conclusão: 2017

Designação do Mestrado: Mestrado em Direito e Informática

Universidade do Minho, __/__/____

Assinatura:

_____

Agradecimentos

Ao meu pai e à minha mãe,

por nunca duvidarem das minhas capacidades,

e por todo o apoio que me deram.

À minha família,

porque mesmo longe, me incentivou a não desistir.

Aos meus amigos,

pelos sorrisos e horas intermináveis de conversa.

Aos meus orientadores,

obrigada pela ajuda e disponibilidade.

Obtenção de Prova Digital: Utilização de *Malware* pelos Órgãos da Polícia Criminal

Resumo: A criminalidade dos nossos dias tem vindo a dissociar-se em absoluto da convencional delinquência, orientada para a lesão de bens jurídicos individuais, manifestando-se agora na prática de atos muitas vezes invisíveis que se traduzem em ofensas a bens jurídicos coletivos. Além disso, com o aperfeiçoamento das técnicas utilizadas para a prática de novas formas de crimes, tais como a cibercriminalidade à escala global, tem crescido o interesse na criação de instrumentos para o combate desta nova forma de criminalidade, principalmente no que diz respeito ao Direito Processual Penal dos Estados.

Assim, e no que nos diz respeito, dentro da área da criminalidade informática, deve-se discutir a utilização de métodos ocultos de investigação criminal, e a possibilidade, à luz do quadro legal e constitucional vigente em Portugal, da possível utilização de *malware* por parte dos órgãos da polícia criminal como meio de obtenção de prova digital, visto que sendo uma área bastante recente, ainda existe pouca legislação, uma grande divergência doutrinal e jurisprudencial, senão uma inexistência destas.

Obtaining Digital Evidence: Use of Malware by Criminal Police Organs

Abstract: Nowadays criminality has been dissociating from conventional delinquency, oriented to the injury of individual legal assets. Now it manifests itself in the practice of acts that are often invisible and which are translated as offenses to collective legal assets. Moreover, with the upgrading of the techniques used for the practice of new methods of crime, such as cybercrime on a global level, there is a bigger interest in the creation of instruments to combat this new form of crime, mostly in the Criminal Procedural Law of States.

Therefore, as far as we are concerned, on the subject of cybercrime, we should discuss the use of hidden methods of criminal investigation, and the possibility of malware being used by the criminal police as a means of obtaining digital proof. Since cybercrime is a recent area, there is still little legislation, a large doctrinal and jurisprudential divergence, if not lack of these.

Índice

Abreviaturas, siglas e acrónimos

AAFDL – Associação Académica da Faculdade de Direito de Lisboa

ADN – Ácido desoxirribonucleico

AJ – Autoridade Judiciária

CARICOM – Comunidade no Caribe

CDADC – Código do Direito de Autor e dos Direitos Conexos

CE – Comissão Europeia

CIPAV – *Computer and Internet Protocol Adress Verifier*

CP – Código Penal

CPP – Código de Processo Penal

CPU – *Central Processing Unit*

CRP – Constituição da República Portuguesa

DCP – Direito Constitucional Penal

DPP – Direito Processual Penal

EUA – Estados Unidos da América

Ex. – Exemplo

FBI – *Federal Bureau of Investigation*

GCHQ – *Government Communications Headquarters*

GMS – Sistema Global para Comunicações Móveis

GNR – Guarda Nacional Republicana

GPS – *Global Positioning System*

HIPCAR – *Harmonization of ICT Policies, Legislation and Regulatory. Procedures in the Caribbean*

HTTP – *Hypertext Transfer Protocol*

IMEI – *International Mobile Equipament Identity*

IMSI – *International Mobile Subscriber Identity*

IP – *Internet Protocol*

ITU – *International Telecommunication Union*

JAI – Justiça e Assuntos Internos da UE

JIC – Juiz de Instrução Criminal

LC – Lei do Cibercrime

LEC – Ley *de Enjuiciamento Criminal*

LOIC – Lei de Organização da Investigação Criminal

MIT – *Massachusetts Institute of Technology*

MP – Ministério Público

NIDS – *Network Intrusion Detection System*

OPC – Órgãos de Polícia Criminal

PJ – Polícia Judiciária

PSP – Polícia de Segurança Pública

RSA – *RSA Data Security*

SEF – Serviço de Estrangeiros e Fronteiros

SMMP – Sindicato dos Magistrados do Ministério Público

SMS – Serviço de Mensagens Curtas

Soca – Serious Organised Crime Agency

ss. – Seguintes

ssl.dll – *Secure Socket Layer Dynamic Link Libraries*

StPO – *Strafprozeßordnung*

TEDH – Tratado Europeu dos Direitos do Homem

TIC – Tecnologias da Informação e Comunicação

TRE – Tribunal Relação de Évora

TRG – Tribunal Relação de Guimarães

TRL – Tribunal Relação de Lisboa

TRP – Tribunal Relação do Porto

UE – União Europeia

USB – *Universal Serial Bus*

VBTS – *Vessel Traffic System*

VS – *Versus*

Introdução

Nos últimos anos, tem-se assistido a um grande avanço das novas tecnologias de informação e comunicação em variadas áreas. Podemos afirmar que quase todos os dias se descobre algo novo, ou há um aperfeiçoamento de uma tecnologia já existente. Tal progresso trouxe claras vantagens e benefício à população em geral, mas também (como todo, o reverso da moeda) desvantagens.

Primeiramente podemos apresentar como vantagens a facilidade de comunicação entre pessoas, que desburocratizou formas de celebrar contratos, principalmente no meio comercial, promoveu um maior acesso por parte da população, dita comum, a notícias e informações, de forma bem acessível em termos económicos. Podemos, pois, considerar que este novo facilitismo de acesso à informação e comunicações é uma das principais causas das transformações económicas, sociais, políticas e culturais. Pode considerar-se o motor da evolução social[1].

Já no que toca às desvantagens, existem algumas desta evolução desenfreada, principalmente no que diz respeito à proteção da vida privada da pessoa humana e também da sua esfera íntima. No que importa ao desenvolvimento do nosso tema, provoca uma discrepância do acompanhamento com manifesta dificuldade de monitorização pelo direito, precisamente pelo direito processual penal.

Assim, sendo uma área bastante recente, é, por vezes, complicado discutir sobre certos temas, dentro da área da criminalidade informática. A divergência doutrinal e jurisprudencial ou mesmo a inexistência destas e a pouca legislação abrem um fosso entre o lícito e o ilícito, de muito difícil resolução. Certos desta realidade, torna-se imprescindível discutir e tratar destas problemáticas da criminalidade informática.

Como tema resolvemos, tratar dos meios de obtenção de prova: uso de *malware* por parte dos órgãos de polícia criminal, no seio da investigação criminal, evidentemente porque se trata de um tema bastante atual, como referimos supra, não havendo um vasto material adequado, torna-se, cada vez mais pertinente, tratar de matérias que se englobam na criminalidade informática de modo a conseguir-se, num futuro, esperamos, próximo, obter uma uniformidade doutrinal e jurisprudencial.

[1] Renato Militão, "A propósito da prova digital no processo penal", Revista da Ordem dos Advogados (Lisboa, 2015), pp. 247-285.

Outra das razões, pela qual escolhemos este tema, é a criminalização de certos ilícitos ter apenas 25 anos, tal como o acesso remoto a um sistema informático, ou os demais previstos na Lei do Cibercrime,[2] comparativamente com outros tipos de ilícitos, há muito tempo punidos como crime. É urgente ultrapassar a dificuldade de, no seio de julgamento não se conseguir provar a prática de crime por parte de certo réu, devido à dificuldade dos meios de obtenção de prova digital.

O recurso a *malware* como meio de obtenção de prova digital revela-se, hoje em dia, bastante útil, pois com o advento das novas tecnologias da informação e comunicação, aliado à facilidade da sua utilização, o combate ao cibercrime torna-se extremamente difícil, sendo que, nas situações de criminalidade mais graves, é urgente a imposição de medidas de carácter mais gravoso.

[2] Lei nº 109/2009 que vem revogar a Lei nº 109/1991 e que apresenta no elenco de crimes, por exemplo a Falsidade Informática, a Sabotagem Informática e o Acesso Ilegítimo.

Delimitação conceptual

1.1.Meios de Obtenção de Prova[3]

No seio do direito processual penal, os meios de obtenção de prova são as diligências efetuadas pelas autoridades judiciárias e policiais para recolha de elementos que, mais tarde, poderão comprovar factos relevantes e levar à conclusão da existência ou não de um ilícito penal, ou seja, são os modos que se efetuam, de forma a reunir indícios que venham a servir para a atividade de recolha de elementos de prova. Tais meios de obtenção de provas podem ser, entre outros, os exames, as revistas e buscas, as apreensões e as escutas telefónicas, sendo as regras gerais destes consagradas nos Capítulos I a IV do Título III do Livro III, nos artigos 171.º a 190.º do CPP.

1.1.1. Exames[4]

Antes de mais, temos de salientar que a noção de exame prevista na lei não se confunde com a etimologia da palavra, ou com o seu sentido corrente, assumindo-se antes de um conceito normativo.

Os exames[5] são uma inspeção cuidadosa do local do crime, reservada à descoberta de vestígios ou provas reais do crime cometido. São um meio de obtenção de prova, a partir do qual se recolhe indícios referentes ao modo de como o crime foi praticado, o lugar onde este decorreu, e ainda as pessoas, quer os sujeitos que cometeram tal crime, bem como sobre quem este foi cometido.

Os exames, e os restantes meios de obtenção de prova (como veremos adiante), carecem de autorização pela autoridade judiciária, contudo, tal autorização depende do consentimento do sujeito a examinar.[6] Em face de recusa limite do sujeito, havendo clara obstrução à obtenção de prova, pode o indivíduo incorrer em crime de desobediência, previsto no artigo 348.º do CP, sendo possível, neste caso, o recurso do uso da força, para a prossecução dos objetivos da investigação. O recurso ao uso da força é sempre, o último recurso, usado, apenas, em situações limites.[7]

---

[3] Francisco Marcolina Jesus, "Os meios de obtenção de prova em processo penal", (Lisboa: Verbo Jurídico, 2015).

[4] Carlos Pinto Abreu, "Prova e meios de obtenção de prova – os exames no processo penal".

[5] Artigos 171.º a 173.º do CPP.

[6] Artigos 270.º nº 1e 249.º nº 2 al.ª a), conjugados com o artigo 172.º nº 2, todos do CPP.

[7] O Acórdão do Supremo Tribunal de Justiça n.º 14/2014 é utilizado como fixação da jurisprudência, no que diz respeito ao crime de desobediência. Apud Carla Jobling e Luís Figueira, "CPP Anotado - Volume II", (JurIndex3, 2015).

Já, no que diz respeito, ao exame sobre características físicas e psíquicas da pessoa, só o juiz pode ordenar, tendo contudo de fundamentar a necessidade da sua realização. Na falta de consentimento do examinado, visto que o número 2 do artigo 172.º, conjugado com o número 2 do artigo 154.º restringe o previsto no número 1 do artigo 172.º. Esta possibilidade é regra geral, podendo ser afastada por regra especial. Pese embora a possibilidade, consagrada na Lei, a integridade física e moral do suspeito, no decorrer de um exame, tem, obrigatoriamente, que ser acautelada.

Podemos enumerar como exemplo de exames, a colheita de vestígios biológicos para a determinação do perfil genético do arguido, ou ainda a análise ao sangue ou urina para a deteção da toxicodependência do arguido.

Entre o exame como meio de obtenção de prova exame e a perícia como meio de prova, há uma distinção que cumpre aqui registar. A perícia requer a perceção e apreciação das matérias recolhidas, assente em conhecimentos técnicos, científicos e artísticos da especialidade (artigo 151.º do CPP). Logo, a figura do perito é essencial no processo.

Assim, na diferenciação, entre o meio de obtenção de prova, que é o exame, e o meio de prova que é a perícia, podemos referir que, no que diz respeito à determinação de um perfil de ADN, que detetar e colher o material biológico é um exame, mas coisa diferente, depois, é, a partir desse material, obter um meio de prova, sendo que a consecução do perfil de ADN, ou seja, a interpretação do resultado alcançado, já é um meio de prova.[8]

1.1.2. Revistas e Buscas

As revistas consistem no exame ou na inspeção meticulosa de uma pessoa, para se verificar se esta oculta ou não objetos que possam estar relacionados com o ilícito penal ou vir a servir de prova daquele. Estas estão previstas nos artigos 174.º e seguintes do CPP e ainda no artigo 251.º do mesmo diploma. Dentro da revista podemos então diferenciar a revista como meio de obtenção de prova (como medida cautelar e de polícia)[9], prevista no artigo 174.º do CPP e a revista como meio de prevenção e/ou de segurança, alínea b) do n.º 1 do artigo 251.º do CPP e também na Lei n.º 8/97 e na Lei n.º 16/04.

[8] Helena Machado e Helena Moniz, "Base da Dados Genéticos Forenses – Tecnologias de Controlo e Ordem Social", (Coimbra: Coimbra Editora, 2014).

[9] Manuel Monteiro Guedes Valente, "Revistas e Buscas", 2.ª edição (Coimbra: Almedina, 2005), página 21.

É importante referir que estas têm de ser autorizadas ou ordenadas pela autoridade judiciária. Tem de haver indícios da existência de quaisquer objetos, relacionados com um crime ou que possam servir de prova, escondidos na própria pessoa, salvo exceções previstas no CPP[10]. O consentimento do visado dispensa a autorização judicial.

Como meio de obtenção de prova encontramos, também, as buscas, sendo que estas se realizam em locais reservados e não acessíveis ao público, onde haja a probabilidade da existência de indícios relacionados com a prática de um crime ou/e que sejam suscetíveis de virem a servir de prova no processo-crime a decorrer.

A busca é portanto, "... a operação desenvolvida pela autoridade judiciária ou por OPC no intuito de obter indícios probatórios para serem carreados para o processo de modo a que se possa prosseguir os fins do processo penal: a realização da justiça através da condenação dos culpados e a absolvição dos inocentes."[11]

Seguindo o princípio constitucional do número 4 do artigo 32.º da CRP as buscas têm de ter autorização judiciária, excetuando os regimes especiais da alínea a) do número 1 do artigo 251.º e do número 4 do artigo 174.º ambos do CPP e ainda o número 3 do artigo 34.º da CRP.

No que concerne às formalidades das revistas e das buscas, podemos reafirmar que ambos os meios de obtenção de prova necessitam, salvo previsão na lei do contrário, de autorização judiciária. Para além disso, o número 1 do artigo 175.º, no caso da revista e o artigo 176.º, no caso da busca, ambos do CPP, obriga a autoridade que preside ou efetua o ato, a entregar uma cópia do despacho autorizador da busca ou revista, ao visado, ou a alguém da sua confiança. No caso da revista, assiste à pessoa de confiança do visado, o direito a presenciar a revista. Já quanto ao caso da realização de busca, o OPC ou a autoridade judiciária competente pela sua realização, é obrigatoriamente, acompanhado pela pessoa de confiança do visado.

1.1.3. Apreensões[12]

As apreensões fazem parte do elenco dos meios de obtenção de prova, e encontram-se previstas nos artigos 178.º a 186.º do CPP. Mais uma vez, dependem de autorização judicial e do cumprimento dos requisitos previstos na lei, por exemplo, a situação da apreensão em escritório de advogados ou consultório médico, segue-se o regido no artigo 180.º. No caso da apreensão da correspondência, esta deve ter sido expedida pelo sujeito ou ter sido dirigida a este. O crime em

[10] Como por exemplo a alínea a) do número 4 do artigo 174.º do CPP.
[11] Valente, "Revistas...", página 61.
[12] Francisco Marcolina Jesus, "Os meios de obtenção...".

causa, tem de ser punível com pena de prisão superior, no seu limite máximo, a três anos e ainda a diligência tem de revelar-se deveras importante para a descoberta da verdade ou para a prova futura.

Consideramos essencial salientar que, existe uma proibição de apreensão de correspondência entre o arguido e o seu defensor[13], excetuando os casos em que há razões, fundamentadas, para se poder crer que a correspondência constitui, ela própria, objeto ou elemento de um crime. Além disso, importa dizer que, este meio de obtenção de prova, em igualdade com os outros, realizado sem ordem ou, sendo o seu consentimento indispensável, é considerado como uma nulidade e uma violação do preceito constitucional do número 8 do artigo 32.º da CRP, sendo que as provas obtidas não podem ser usadas, ou seja, estamos perante uma nulidade insanável.

1.1.4. Escutas telefónicas[14]

Encontramos no elenco de meios de obtenção de prova as escutas telefónicas, estando estas consagradas nos artigos 187.º e seguintes do CPP. Podemos defini-las, como a interceção e a gravação de conversações ou comunicações telefónicas, entre os presumíveis suspeitos de certos crimes, previstos no catálogo do número 1 do artigo 187.º do CPP. E mais uma vez, por estarmos perante um caso de restrição de Direitos, Liberdades e Garantias permitido pelo número 2 do artigo 18.º da CRP e o número 4 do artigo 34.º *a contrario* do mesmo diploma[15], é expressamente necessária a autorização judicial para a execução da escuta telefónica por parte dos OPC, correndo o risco de se tal não acontecer, estarmos perante um meio de obtenção de prova proibido.

Aos OPC, cabe, assim, a execução da escuta e também a elaboração do auto, ou seja, da transcrição do conteúdo áudio relevante para a prova. É também responsabilidade de descrever de modo sucinto tal conteúdo e explicar o seu alcance para se a chegar à descoberta da verdade material. O MP tem o poder de mandar os OPC transcrever as escutas telefónicas, como verificamos na alínea a) do número 9 do artigo 188.º do CPP. Contudo, como apuramos nas restantes alíneas deste mesmo número, dá-se agora, a possibilidade ao arguido e ao assistente, de fazer a transcrição por meios próprios.

[13] Segredo profissional, previsto no artigo 182.º do CPP.

[14] Ferreira Marques, "Meios de Prova", In: Jornadas de direito processual penal. O novo código de processo penal. – (Coimbra: Almedina, 1988), pp. 219-270.

[15] O domicílio e o sigilo da correspondência e de outros meios de comunicação privada são invioláveis, além de que é proibida toda a ingerência das autoridades públicas na correspondência e nas telecomunicações, exceto quando a lei penal consagre o contrário.

1.2 Meios de prova vs meios de obtenção de prova

Cavaleiro de Ferreira[16] afirma que "o fim da prova é a demonstração da verdade dos factos", ou seja, tem como principal fim a descoberta da verdade material, da verdade que mais proximamente corresponde ao acontecer histórico dos factos.

Assim, analisaremos primeiramente, alguns princípios fundamentais no processo penal, que consideramos pertinentes a este tema.

O princípio de investigação, ou da verdade material, traduz-se no poder dever, que ao tribunal cabe de proceder oficiosamente (ou a requerimento), à produção de todos os meios de prova, cujo, conhecimento lhes afigure essencial à descoberta da verdade e à boa decisão da causa.[17]

Além, do dever de atender aos meios de prova oferecidos, em tempo oportuno, pela acusação e pela defesa, pode o juiz ordenar a produção de mais meios de prova, como se consagra no número 2, do artigo 340.º do CPP.[18]

No âmbito da audiência de julgamento, este princípio verifica-se de forma limitada, uma vez que, o princípio da vinculação temática[19] restringe os poderes de cognição do juiz, proibindo-o de investigar os fatos que se afastem do objeto do processo. Além disso, a produção probatória encontra-se também sujeita aos limites impostos, nomeadamente, pelo artigo 126.º do mesmo diploma, e o número 8 do artigo 32.º da CRP.

Achamos, importante referir, que e segundo Figueiredo Dias[20], em processo penal, "não está em causa a verdade formal, mas a verdade material, que há-de ser tomada em duplo sentido: no sentido de uma verdade subtraída à influência que, através do seu comportamento processual, a acusação e a defesa queiram exercer sobre ela: mas também no sentido de uma verdade, que não sendo absoluta ou ontológica, há-de ser antes de tudo uma verdade judicial, prática e sobretudo, não uma verdade obtida a todo o preço mas processualmente válida."

Já, o princípio do contraditório, de acordo com a 2ª parte, do n.º 5 do artigo 32.º da CRP, e também do número 2, do artigo 327.º do CPP, afirma que a audiência de julgamento e os atos instrutórios que a lei determinar, devem, dentro do processo criminal, ter sempre em conta, de forma igual, as razões da acusação e, também, as da defesa. Além disso, o juiz deve ouvir, sempre, todos os participantes processuais, para tomar qualquer decisão que pessoalmente os atingem.

---

[16] Manuel Cavaleiro de Ferreira, "Lições de Direito Penal - Parte Geral I – II", (Coimbra: Almedina, 2010).
[17] Como por exemplo, os artigos 323.º, alíneas a) e b) e 340.º, n.º1, ambos do CPP.
[18] Paula Marques Carvalho, "Manual Prático de Processo Penal, 10.ª edição", (Coimbra: Almedina, 2017).
[19] Segundo o qual, toda a atividade probatória a realizar, tem como limite os factos que constam da acusação ou da pronúncia.
[20] Jorge Figueiredo Dias, "Clássicos Jurídicos - Direito Processual Penal", (Coimbra: Coimbra Editora, 2004).

Este princípio é uma garantia processual, dada a todo o sujeito afetado por uma decisão. Sendo esta garantia, consagrada numa prévia audição deste, e de, assim, ser possível, trazer-se ao processo, todos os elementos necessários à decisão, contribuindo ativamente para que o tribunal possa, vir a decidir acertadamente.

Os meios de prova são os elementos que permitem afirmar a realidade dos factos relevantes para a existência ou não do ilícito criminal, a punibilidade ou não punibilidade do arguido e a determinação da sanção aplicável. São, por si mesmos, fonte de convencimento do tribunal. É, portanto, com base nestes elementos que as autoridades competentes, especialmente os tribunais, baseiam algumas das suas decisões, incluindo a de condenação ou absolvição do sujeito. A prova é apreciada segundo as regras da experiência e a livre convicção da entidade competente.

Segundo Antunes Varela, Miguel Bezerra e Sampaio Nora, os meios de prova são os elementos de que o julgador se pode servir para formar a sua convicção acerca de um facto.[21]

Os meios de utilização mais comum são:

- a prova testemunhal;

- as declarações do arguido, do assistente e das partes civis;

- a prova por acareação, que é um confronto entre sujeitos que prestaram declarações contraditórias;

- a prova por reconhecimento, ou seja, a identificação e/ou descrição de uma pessoa por parte de outra;

- a reconstituição do facto, a reprodução, tão fiel quanto possível, das condições em que se afirma ou se supõe ter ocorrido o crime e a repetição do seu modo de realização;

- a prova pericial e

- a prova documental.

Assim, dentro dos meios de prova, podemos subdividi-los em dois subtipos: em primeiro as provas pessoais, as quais resultam dum ato de pessoa, ou seja, quando o homem é o meio de obtenção de prova. Elencamos, aqui, a prova pericial e a prova por declarações e a prova testemunhal. No segundo subtipo, encontramos as provas reais, sendo elas, a prova por acareação, reconhecimento, a prova documental e ainda os vestígios e indícios.

Este último tipo de meio de prova, os vestígios e indícios, carateriza-se pela especificidade, de os seus meios de obtenção de prova serem regulados pelo legislador, e encontrarem-se

[21] Antunes Varela, *et al.*, "Manual de Processo Civil", (Coimbra: Coimbra Editora, 2004) página 452.

consagrados nos artigos 171.º a 190.º do CPP, sendo estes os que relevam para a matéria em análise.

Diversamente, os meios de obtenção de prova são as diligências realizadas pelas autoridades para recolher a prova. Portanto, são instrumentos de que se servem as autoridades, responsáveis pela investigação criminal, para investigar e recolher meios de prova. Os meios de obtenção de prova mais tradicionais são portanto elencados nos artigos referidos no parágrafo anterior.

Os meios de obtenção de prova são os instrumentos de que se servem as autoridades judiciárias para investigar e recolher meios de prova, afirma Germano Marques da Silva.[22]

No processo penal português, são admissíveis todas as provas que não forem proibidas por lei. E a lei, em conformidade com a Constituição, proíbe as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas, bem como, ressalvados alguns casos previstos na lei (por exemplo, as buscas domiciliárias ou as escutas telefónicas), as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento da pessoa visada.

1.3 *Malware*

Malware[23] é uma junção de dois conceitos. Sendo eles o *software* e malicioso. Assim, no que diz respeito ao *malware* este é um *software* que tem como principal função, infiltrar-se num sistema informático alheio e de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações, e ainda tem o poder de perturbar o normal funcionamento do sistema informático infecionado.

Existem variadas formas em que este pode aparecer, desde o acesso à internet e a sua "comum" utilização (via sites hackeados, demos de *games*, arquivos de música, barras de ferramentas, *software*, entre outros) ou desde um código executável, a *scripts* de conteúdo ativo, e ainda outros *softwares*.

Portanto, podemos dizer que *malware* é o termo utilizado quando nos estamos a referir às várias formas de *software* hostil, intrusivo ou maligno. Em resumo, podemos elencar como principais tipos de malware e que mais se relacionam com o nosso tema: o *Trojan* (Cavalo de

[22] Germano Marques Silva, "Curso de Processo Penal II", (Lisboa: Verbo, 2011), página 209 a 210.
[23] John Aycock, "*Computer Viruses and Malware*", (EUA: Springer, 2007), página 2 e ss..

Troia), Vírus, *Worm*, *Keylogger*, *Spyware*, *Sniffers*, *Bot* e *Rootkit*. Existindo ainda, *Screenlogger*, *Adware*, *Backdoor*, *Exploits*, *Port Scanners* e *Quantum*.

1.4 Órgãos de Polícia Criminal

Órgãos de polícia criminal são as entidades ou agentes policiais que, ou praticam um ato processual penal, ou atuam sob direção de uma autoridade judiciária.[24] Os OPC estão inseridos num ramo maior da Administração Pública, que tem como principal função defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos, conforme preceituado no artigo 272.º da CRP. Os mais conhecidos são: Polícia Judiciária (PJ), Polícia de Segurança Pública (PSP), Guarda Nacional Republicana (GNR) e Serviço de Estrangeiros e Fronteiras (SEF), como verificamos no artigo 3,º da LOIC.

A principal justificação para o aparecimento da atividade policial foi a necessidade de garantia da manutenção da ordem pública e a preservação da segurança e tranquilidade pública. Podemos considerar que os OPC, têm como função estas tarefas, podendo ser acrescentadas, ainda, a luta contra a criminalidade e a prevenção dos crimes.

A CRP, do ponto de vista funcional, dá um sentido unitário a toda a atividade policial, conforme o que já referimos no parágrafo anterior e encontramos consagrado no número 1 do artigo 272.º deste diploma. Já do ponto de vista orgânico, o texto constitucional coloca a Polícia dentro da chamada administração executiva.

A competência dos OPC, encontra-se consagrada nos artigos 4.º e seguintes, da Lei n.º 49/2008, de 27 de agosto.

Em suma, os órgãos de polícia criminal são aquela parte das forças policiais que, têm como principais tarefas, a prevenção criminal e a repressão penal. Dito de forma mais geral, a luta contra a criminalidade. Assim, os OPC conseguem assegurar a interpenetração e fungibilidade presente nestas duas tarefas.

[24] Manuel Monteiro Guedes Valente "Dos Órgãos de Polícia Criminal - Natureza; Intervenção; Cooperação", (Coimbra: Almedina, 2004)

1.5 Investigação Criminal

Em primeiro lugar, cabe-nos definir investigação, como sendo as metodologias que os órgãos responsáveis, estabelecem com a finalidade de obtenção de provas e contraprovas, funções adjuvantes na reformulação de hipóteses e na preparação de novos passos, necessários à prossecução do infindável processo de reajustamento, entre a teoria, a hipótese e o caso concreto, ou seja, o motivo da pesquisa.[25]

A investigação criminal, tem como principal fundamento a procura da verdade dos factos que originaram a realização de um ilícito criminal, a sua análise, e também o estudo do criminoso, da vítima e do controlo social. Assim, podemos definir investigação criminal como o processo de procura de indícios ou/e vestígios, que indiquem e expliquem quem, como, quando, onde e porquê certo crime foi cometido.

Gomes Dias afirma que a investigação criminal "descobre, recolhe, conserva, examina e interpreta as provas reais", assim como "localiza, contacta e apresenta as provas pessoais" que conduzam ao esclarecimento da verdade material dos factos que consubstanciam a prática de um crime.[26] Assim, "a investigação criminal quer-se científica, metódica e integrante de um pensar de ser humano centro de toda a discussão produzida pela ciência de modo a que mais do que objeto seja sujeito ativo e transformador de um mundo do tempo em constante passado."[27]

Em suma, a investigação criminal tem como fim último a aplicação do direito nas prossecuções de defesa da sociedade, do coletivo, de modo a garantir ordem social, liberdade e segurança e direitos inalienáveis.

1.6 Criminalidade Informática

Cibercriminalidade é um conceito recente, que entrou no nosso ordenamento jurídico com a Lei n.º 109/2009, que transpôs para a nossa ordem jurídica a decisão quadro n.º 2005/222/JAI, do CE, relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção de Budapeste.

Garcia Marques e Lourenço Martins alertavam para a inexistência de um conceito de "criminalidade informática" expressamente consagrado na legislação, ou uniformemente

[25] Lei n.º 49/2008 de 27 de agosto, que revogou a Lei nº 21/2000 de 10 de agosto.

[26] Posição tomada num debate que ocorreu em 1981 sobre A Revisão Constitucional, o Processo Penal e os Tribunais, organizado pelo SMMP *apud* Teresa Pizarro Beleza e Frederico Isasca, Direito Processual Penal Textos, AAFDL, Lisboa, 1992, p. 65.

[27] Manuel Monteiro Guedes Valente, Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias", página 473 e 474.

sedimentado na doutrina e jurisprudência. Ainda que, com a Lei n.º 109/1991 falava-se de criminalidade informática como "todo o ato em que o sistema informático serve de meio para atingir um objetivo criminoso ou em que o sistema informático é o alvo simbólico desse ato ou em que o sistema informático é o objeto do crime[28]." É, ainda, "incontornável reconhecer que as realidades sociológicas de tipo criminógeno atualmente discutidas a propósito do cibercrime estão muito para lá daquilo que na lei portuguesa se consagrou como criminalidade informática."[29]

Esta definição levanta, portanto, algumas dicotomias que dificultam a consagração de um conceito uniforme de "criminalidade informática", sendo que nos faz diferenciar dois tipos de criminalidade informática.

O primeiro tipo é a criminalidade informática em sentido amplo, sendo que esta engloba toda a atividade criminosa que pode ser levada a cabo por meios informáticos. Estes podem ser apenas um meio ou instrumento para a prática do ato, ou seja, podem não fazer parte do tipo legal (o crime pode ser praticado com recurso a outros meios). No segundo tipo, referimos a criminalidade informática em sentido estrito. Esta compreende aquele conjunto de tipos legais de crime, que introduzem um meio informático ou um elemento digital no tipo legal de crime, ou ainda, a informática faz parte do objeto tutelado por este tipo legal de crime.

Como exemplo da primeira forma de criminalidade informática podemos elencar o crime de injúria ou de difamação *online*[30], onde as TIC são apenas o meio para divulgar a expressão injuriosa ou difamatória. Já, no que diz, respeito à criminalidade informática em sentido estrito, podemos enumerar a falsidade informática, a sabotagem informática e o acesso ilegítimo.

Podemos afirmar que existiram e ainda existem variadas tipologias classificatórias de criminalidade informática usadas pela doutrina. Em primeiro lugar, referimos E.J. Lampe que partindo do critério sistematizador vinculado às caraterísticas do processamento automático de dados e uma separação dos diversos tipos criminológicos de conduta, agrupou as condutas mais significativas em cinco modalidades, sendo exemplo dessas a manipulação de dados e/ou programas, ou mais precisamente a "burla informática" e a cópia ilegal de programas[31].

Nomes como Ulrich Sieber, Davara Rodriguez, Rovira del Canto, Faria Costa e Helena Moniz, também propuseram uma posição no que diz respeito a este conceito.[32] Mas relevando

[28] Garcia Marques e Lourenço Martins, "Direito da Informática", 2.ªediçao, (Coimbra: Almedina, 2006).

[29] Pedro Verdelho, " Cibercrime", In Direito da Sociedade da Informação – Vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra: Coimbra Editora, 2003), página 347.

[30] Artigos 180.º e 181.º do CPP.

[31] Apud Benjamim Silva Rodrigues, "Direito Penal – Parte Especial – Tomo I – Direito Penal Informático-Digital" (Coimbra: Coimbra Editora, 2009), página 169.

[32] Apud Benjamim Silva Rodrigues, "Direito Penal – Parte Especial...", páginas 169 e ss..

para a nossa dissertação, analisamos a posição de José Oliveira Ascensão, que considera a relevância jurídico-penal do meio informático como fator determinante da existência da criminalidade informática. Procede, em conformidade, à caracterização dos tipos legais de crime, baseados:

Em primeiro lugar no uso de instrumentos informáticos, considerando na qualificação dos tipos comuns pelo meio informático a burla informática e o dano informático (artigo 221.º do CPP e artigo 5.º do CP, respetivamente). Considera estes dois tipos de crime como desenvolvimento dos elementos delimitadores já previstos na legislação penal, artigos 217.º e 212.º do CP, respetivamente.

Em segundo lugar na agressão ao meio informático, integra os tipos cujos objetos são meios informáticos, aqui se produzindo a criação de novos tipos penais. E por fim, no conteúdo da mensagem deixada disponível em rede.

2. CAPÍTULO I

Meios de obtenção de prova digital em Processo Penal

2.1 Tipos de dados informáticos

Consideramos importante, antes de iniciar este capítulo sobre meios de obtenção de prova digital, fazer uma distinção da tipologia e conceito de dados de comunicação existentes, visto que, hoje, se exige aos operadores de telecomunicações, que estes guardem os dados durante um período de tempo e que quando estes sejam pedidos pela autoridade judicial ou pelo órgão de polícia criminal (sempre com a autorização judicial necessária), venham a ser-lhes facultados, conforme o plasmado nos artigos 4.º e 5.º da Lei nº 32/2008 de 17 de Julho, que transpôs para a ordem jurídica interna a Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março e ainda o artigo 12.º da LC.

A alínea b) do artigo 2.º da LC define dados informáticos como "qualquer representação de factos, informações ou conceitos sobre uma forma suscetível de processamento num sistema informativo, incluindo os programas aptos a fazerem um sistema informático executar em função". Logo, se estivermos perante um documento eletrónico, um programa de sistema informático, dados pessoais ou ainda dados de tráfego ou localização, todos estes são considerados dados informáticos.

Dentro destes, podemos distinguir quatro categorias:

- A primeira são os dados de localização, estes, caracterizam-se por indicar-nos a localização geográfica do equipamento terminal de qualquer utilizador de um serviço de comunicações eletrónicas publicamente disponível. Ainda, indicam-nos a origem e o destino de uma comunicação.

- Em segundo lugar encontramos os dados de tráfego. Podemos considerar que nesta categoria deparámo-nos com os dados informáticos ou técnicos, relacionados com uma comunicação realizada por meio de tecnologias de comunicação e informação, por si gerado, mencionando, nomeadamente, a origem da comunicação, a hora e a data, os trajetos, o tamanho e ainda a duração ou o tipo de serviço subjacente.

- A terceira categoria consideramos os dados de base, sendo estes os dados pessoais, que tem a ver com a conexão à rede de comunicações. O número, a morada ou a identidade do assinante, são, materialmente, os elementos desta categoria.

- Em último lugar, podemos distinguir os dados de conteúdo, que são como o nome indica, os dados relativos ao conteúdo de uma comunicação ou de uma mensagem.

Concluída esta distinção, podemos agora afirmar que os dados de tráfego são a origem e sustentação de todos os outros. Para além disso, cabe-nos asseverar que os dados de tráfego e de localização, podem, no âm*bit*o da investigação criminal ser solicitados pelas autoridades de polícia criminal e/ou judiciárias. Mais, verificando-se a recusa de atender a solicitação, como acontece com alguns meios de obtenção de prova, podem os operadores de telecomunicações, incorrer em crime de desobediência. No que diz respeito aos dados de bases, a única forma de não se permitir o acesso a estes é que o titular desses dados se manifeste, de forma expressa, contra a sua publicidade. Esta prerrogativa assenta no clausulado do contrato celebrado entre os utilizadores e os operadores de telecomunicações. Finalmente, o regime de dados de conteúdo tem um tratamento igual ao regime geral dado às escutas telefónicas, previsto nos artigos 187.º a 189.º do CPP.

2.2 Obtenção de prova digital

A obtenção de prova digital[33] é bastante difícil devido a variados fatores. Em primeiro lugar podemos referir o anonimato da informação digital, afirmando assim, que esta é uma sequência de codificação de dígitos desenvolvendo um conhecimento. Logo, a codificação é o significado dos dígitos decidido pelo contexto em que a informação é gerada e utilizada. Não podemos encontrar na informação digital gerada, armazenada e transmitida entre os dispositivos qualquer ligação física com a pessoa enquanto indivíduo a que os dados possam pertencer. Tal dificulta, muitas vezes, a autorização necessária para se chegar a certos meios de obtenção de prova, apesar de se tratar de uma situação concreta e individual e não abstrata e geral. Além disso, o próprio carácter técnico deste tipo de condutas criminosas apresenta mais uma dificuldade no que diz respeito à obtenção de prova.

[33] A prova digital "pode definir-se como qualquer tipo de informação, com valor probatório, armazenada (em repositório eletrónico-digitais de armazenamento) ou transmitida (em sistemas e redes de comunicações eletrónicas, privadas ou publicamente acessíveis), sob forma binária ou digital." Renato Lopes Militão, "A propósito da prova digital...", página 259.

Igualmente importante, é referir o perigo que existe de se encontrar informação danificada. O uso de dispositivos de armazenamento incompetentes. A humidade, a radiação ultravioleta, a danificação, nem que seja apenas de um bit, podem causar alterações gravíssimas o material probatório e inviabilizar o uso do meio da descoberta da verdade, no seio do processo penal.

A obtenção de prova digital e os meios utilizados para tal é considerada, bem como os meios de obtenção de prova "tradicional", intrusiva na vida pessoal dos visados e, por isso, estamos perante ofensas aos Direitos, Liberdades e Garantias consagrados na CRP. O recurso utilizado pelas OPC e JIC em ordem a descobrirem a verdade material e conseguirem concluir sobre a autoria de um ilícito criminal, deve ser utilizado de forma apropriada, apenas quando for absolutamente indispensável, na justa medida e proporcionalidade, sem nunca ultrapassar o limite necessária à obtenção da prova, como previsto no número 2 do artigo 18.º da CRP. Ainda, as restrições aos direitos fundamentais carecem sempre de justificação, sendo esta a ideia de salvaguarda de outros direitos ou interesses constitucionalmente protegidos superiores aos que vão ser restringidos por estas medidas. Por isso, a importância de que apenas com o consentimento do visado ou com autorização judicial, se pode dar uso a qualquer meio de obtenção de prova, seja ele digital ou "tradicional", tem que ser uma certeza[34].

Importa, aqui, salientar que as escutas telefónicas, os pedidos de obtenção de dados de tráfego e os pedidos de localização celular, exemplos dos meios de obtenção de prova digital, têm, sempre, como alvo, um suspeito em concreto, nunca podendo se considerar que a recolha de informações de um número abstrato de pessoas seja proporcional com o consagrado no artigo 18.º da CRP. A falta da determinabilidade de um suspeito é, pois, um obstáculo intransponível para a realização dos meios de obtenção de prova digital. Temos, apenas, de apresentar como exceção a esta regra, o preceituado na Lei n.º 32/2008, de 17 de Julho, visto que os "dados pessoais, gerados e conservados, no âmbito de uma comunicação eletrónica ou serviços de comunicações eletrónicas, a partir das redes de comunicações eletrónicas publicamente acessíveis, se encontram, agora, depositados, durante um longo período de tempo, à ordem do Estado Português".[35]

[34] Benjamim Silva Rodrigues, "Da Prova Penal – Tomo II – Bruscamente... A (s) Face (s) Oculta (s) dos Métodos Ocultos de Investigação Criminal", (Lisboa: Rei dos Livros, 2010), páginas 51 e ss..

[35] Benjamim Silva Rodrigues, "Direito Penal - Parte Especial - Tomo I - Direito Penal Informático-Digital", (Coimbra: Coimbra Editora, 2009), página 695.

2.2.1 Lei do Cibercrime

O artigo 11.º da LC afirma que o elenco de crimes, nos quais se pode obter prova digital, são os previstos na lei em análise, ou seja, são cometidos por meio de um sistema informático ou os ilícitos criminais, em relação aos quais seja, necessário proceder à recolha de prova em suporte digital.

Estamos perante uma criação de meios de obtenção de prova para combater diretamente a criminalidade, seja qual for a sua forma. Atendendo à generalização do uso de meios informáticos no quotidiano, à necessidade de adaptação do combate ao crime, e mais precisamente dos meios de obtenção de prova a esta realidade, impõe-se um gigantesco trabalho, neste âmbito.

Na Lei do Cibercrime, Lei nº 109/2009, de 15 de setembro, é, então, consagrada a possibilidade de obter prova digital no decurso de uma investigação criminal, no que diz respeito às medidas de "preservação expedita de dados" (artigo 12.º), "revelação expedita dos dados" (artigo 13.º), "injunção para apresentação ou concessão de acesso a dados" (artigo 14.º), "pesquisa de dados informáticos" (artigo 15.º), "apreensão de dados informáticos" (artigo 16.º), "apreensão de correio eletrónico e registos de comunicações de natureza semelhante" (artigo 17.º). Encontramos ainda duas formas de combate a um número mais pequeno de crimes, dois tipos de meios de obtenção de prova, são eles "interceção de comunicações" (artigo 18.º) e "ações encobertas" (artigo 19.º). Nunca esquecer, que as normas referentes aos meios de obtenção de prova digital devem estar inseridos no regime geral dos meios de obtenção de prova, com as devidas alterações atendendo às suas particularidades.[36]

Os artigos 12.º a 17.º da Lei do Cibercrime podem ser aplicados como um todo, pois representam um conjunto integrado de medidas processuais, onde os aspetos práticos deles se relacionam e complementam-se.

A preservação expedita de dados (artigo 12.º da LC) deve ser ordenada pela autoridade judiciária competente, a quem tem a disponibilidade ou controlo dos dados informáticos, normalmente o fornecedor de serviço. Esta ordem de preservação dos dados destina-se ao acautelamento ou prevenção da perda, deterioração ou modificação dos respetivos dados, sendo que tal, inviabilizaria toda e qualquer investigação ou procedimento criminal a decorrer. Importa salientar, que no caso de urgência ou perigo na demora os OPC podem ordenar a preservação dos dados e também, podem fazê-lo, mediante autorização da autoridade judiciária (número 2 do

[36] Pedro Dias Venâncio, "Lei do Cibercrime: Anotada e Comentada" (Coimbra: Almedina, 2011).

artigo 12.º da LC). Finalmente, sobre este artigo, referimos que os dados não são preservados e guardados para sempre. Há um período de tempo máximo de três meses, sendo que este pode ser renovado, até um máximo de um ano, conforme previsto na alínea c) do número 3 do artigo 12.º e o número 5 do mesmo artigo.

O artigo 13º da LC, consagra a revelação expedita de dados de tráfego, sendo que, logo que o fornecedor de serviço souber a quem a preservação de dados foi ordenada, tem de indicar ao OPC ou a AJ[37], os "outros fornecedores de serviço através dos quais aquela comunicação tenha sido efetuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efetuada."[38] Cabe-nos ainda referir, no que diz respeito a esta matéria, o princípio da suficiência. Tal princípio, expressa um entendimento quantitativo, pois, apenas valerá a transmissão de dados, cuja quantidade se revele suficiente, para os efeitos pretendidos pela investigação criminal.

Muitas vezes, cada um dos fornecedores de serviços não detêm os dados de tráfego em número suficiente para possibilitar a identificação da verdadeira origem ou destino da comunicação em investigação. Após a divulgação deste tipo de dados, pode a autoridade judiciária ou os órgãos de polícia criminal, identificar quaisquer outros fornecedores de serviços, e, ainda, o caminho através do qual a comunicação foi transmitida.

Ainda na matéria dos dados e da sua preservação e revelação expedita, surge-nos agora o artigo 14.º da LC, que prevê a injunção para apresentação ou concessão do acesso a dados. Tendo sempre em conta a descoberta da verdade material e a ideia de justiça, pode, no decurso do processo, ser necessário a produção de prova, obtendo dados informáticos específicos e determinados, armazenados num determinado sistema informático, sendo que a autoridade judiciária competente, mais uma vez, ordena a quem tenha a disponibilidade ou o controlo sobre esses dados que os comunique ao processo e, permita o acesso a estes, às entidades competentes.

Este artigo é aplicado aos fornecedores de serviço que, se não cumprirem tal ordem, incorrem na pena de punição por desobediência. Sendo que a estes, pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma

[37] Benjamim Silva Rodrigues, "Da Prova Penal – Tomo II...", página 444.
[38] Artigo 13.º parte final, LC.

de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, conforme o assente nas alíneas do numero 4 do artigo em questão.[39]

Por último, no que diz respeito ao uso da injunção prevista neste artigo, cabe-nos salientar que o sigilo decorrente de certas profissões, tais como médicos, advogados e jornalistas, leva a que os sistemas informáticos utilizados no seio destas profissões, não possam ser objetos utilizados com a base neste artigo.

Na descoberta da verdade, pode ser necessário dentro do processo, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, como consagra o artigo 15.º da Lei do Cibercrime. Estamos, pois, perante uma pesquisa nesse sistema informático. Salientamos, que é necessária a autorização da autoridade judiciária, a qual deve, sempre que possível, presidir à diligência em questão. Só nos casos previstos na lei, os OPC podem proceder a tal pesquisa, ou seja, quando esta for consentida de forma voluntária, por quem tiver o controlo ou a disponibilidade dos dados e, esse consentimento ficar documentado. Podemos afirmar ainda, que os OPC podem efetuar uma pesquisa, nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime, que ponha em grave risco a vida ou a integridade de qualquer pessoa (alíneas a) e b) do número 3 do artigo 15.º do diploma acima referido). Torna-se também importante referir que, caso os OPC procedam à pesquisa de dados informáticos devem comunicar imediatamente à autoridade judiciária competente, sob pena de nulidade da diligência. Além disso, há lugar à elaboração e envio de um relatório resumido, mas detalhado, onde mencionam as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e das provas recolhidas. [40]Ainda no que diz respeito ao artigo 15.º, podemos afirmar que são aplicáveis as regras, sempre com as devidas adaptações, das buscas.

No decorrer duma pesquisa informática ou de outro acesso legítimo a um sistema informático, se forem encontrados dados ou documentos informáticos que sirvam como prova e que levem à descoberta da verdade material, deve a autoridade judiciária competente, autorizar ou ordenar por despacho a apreensão destes. Assim o prevê o artigo 16.º da LC. Os órgãos da polícia criminal podem efetuar as apreensões sem que haja prévia autorização da autoridade judiciária, no decurso da pesquisa informática decorrente do artigo número 15.º do mesmo

[39] "a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;
b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou
c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível como base num contrato ou acordo de serviços.".

[40] Artigo 253.º CPP.

diploma. Podem, ainda, em situações de urgência ou perigo, como sejam a perda ou deterioração dos dados, quando haja demora da obtenção da autorização da AJ. Caso estejamos perante conteúdos que possam revelar dados pessoais ou íntimos suscetíveis de produzir tais efeitos, serão apresentados ao juiz, que apreciará sobre a junção destes, ou não, aos autos. Mais uma vez, e como de todas as remanescentes vezes já referidas, estamos perante uma área de direitos e interesses legalmente protegidos, que apenas poderá ser restringida em casos bastantes específicos.[41]

Podemos então apresentar quatro tipos de apreensão de dados informáticos, tal como prevê-se nas alíneas do número 7 do artigo referido no parágrafo anterior:

"a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura;

b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos;

d) Eliminação não reversível ou bloqueio do acesso aos dados."

Como já referimos, o artigo 17.º da LC, prevê a apreensão de correio eletrónico e dos registos de comunicações de natureza semelhante, nas situações em que no decurso de uma pesquisa informática, ou outro acesso legítimo a um sistema informático, forem detetadas ou armazenadas nesse sistema informático, ou noutro a que seja permitido o acesso legítimo, a partir do primeiro.

Podemos equiparar tal meio de obtenção de prova, com o previsto no artigo 179.º do CPP, ou seja, caso o arguido autorize e dê o seu consentimento, pode obter-se através da apreensão (por exemplo de *SMS*) prova necessária para a descoberta da verdade material. Caso o consentimento não suceda, tal como na apreensão da correspondência, é necessário recorrer-se a autorização judicial, sendo esta sempre justificada e adequada. Além disso, o juiz deve ser sempre a primeira pessoa a tomar conhecimento do conteúdo da apreensão. Se tal não acontecer, podemos considerar, que se incorre na obtenção de prova proibida e, consequentemente na pena de nulidade.

[41] A restrição de direitos, liberdades e garantias tem de revestir carácter geral e abstrato, e não pode ter efeito retroativo, nem diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais, além de que só pode acontecer tal restrição nos casos previstos na lei e ancorados na lei constitucional, devendo estas restrições limitarem-se ao mínimo necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos, como verificamos no artigo 18.º da CRP.

A apreensão de SMS, de correio eletrónico ou de comunicação de idêntica natureza, merecem o mesmo enquadramento legal, inserindo-se todas no artigo 17.º da LC.[42] As SMS deixam de se considerar uma comunicação em transmissão, para começarem a ser uma comunicação já recebida. Isto é, a mesma essência da correspondência. Neste caso, não há distinção entre estas (as SMS e o correio eletrónico ou comunicação de idêntica natureza estão em pé de igualdade com a "carta remetida por correio físico"). Tendo o seu destinatário total disponibilidade para difundir o seu conteúdo, ou consentir que destas, as autoridades policiais ou judiciais tomem conhecimento, estamos, neste caso, perante o consentimento do visado.[43] Há ainda a referir que, o facto de as SMS terem sido ou não abertas e lidas ou não pelo destinatário, não é relevante para a matéria em apreço.[44]

Já no que diz respeito à apreensão de correio eletrónico ou ao registo de comunicações de natureza semelhante, a LC, ao remeter para o regime geral de obtenção de prova previsto no CPP, determina a aplicação deste regime na sua totalidade, sem redução do seu âmbito. Uma vez mais, reforçamos o recurso à autorização ou determinação por despacho judicial, deste meio de obtenção de prova digital (tal como todos os outros), devendo, ainda, o juiz ser o primeiro a tomar conhecimento sobre o conteúdo da apreensão, sob pena de nulidade. Pode o MP ordenar uma pesquisa de dados informáticos, resultando desta a apreensão de SMS ou correio eletrónico, contudo, depois deve esta ser autorizada pela autoridade judicial, ou seja, embora o MP deva tomar conhecimento em primeiro lugar das mensagens, ordenando a apreensão provisória, para não se perder a utilidade da prova, o JIC deve ordenar a apreensão definitiva[45].

Podemos afirmar que ao MP cabe a competência para fazer o pedido de identificação de um cliente que utilizou certo endereço IP, num determinado dia e hora, ao operador de comunicações. Contudo, se estivermos perante um pedido, onde se pretenda obter todos os dados do utilizador do IP, num certo período de tempo, neste caso já é necessária a autorização judicial, porque estamos perante dados de tráfego e não apenas dados de base.

A LC consagra, portanto, os meios de obtenção de prova digital e assim, no artigo 18.º do diploma em questão, podemos verificar que se permite o recurso à interceção de comunicações em processos relativos a crimes previstos nessa mesma lei. Salientamos ainda que se aplica a crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário

[42] Benjamim Silva Rodrigues, "Da Prova Penal – Tomo II...", páginas 453 e seguintes.
[43] Acórdão do Tribunal de Relação de Lisboa, de 24 de setembro de 2013.
[44] Acórdão do Tribunal da Relação do Porto, de 12 de setembro de 2012.
[45] Acórdão do Tribunal da Relação de Guimarães, de 29 de março de 2011.

proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do CPP, sendo estes os crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos; relativos ao tráfico de estupefacientes; de detenção de arma proibida e de tráfico de armas; de contrabando; de injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone; de ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou de evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores.[46]

A interceção pode ter como destino a recolha e registo de dados de tráfego, mas, contudo, podemos ir mais além e esta destinar-se, também, aos dados relativos ao conteúdo das comunicações. Esta diligência tem de estar de acordo com as necessidades concretas da investigação e nunca passar esse limite. A violação de direitos e interesses legalmente protegidos, que decorre desta diligência, faz com que apenas quando é indispensável para a descoberta da verdade ou em que a prova seria, de outra forma, impossível ou muito difícil de obter, seja utilizada a interceção e o registo de transmissões de dados informáticos, durante a fase de inquérito, e apenas, com a autorização de um despacho fundamento pelo JIC, mediante requerimento do MP, como verificamos com o numero 2 do artigo 18.º da LC.

Igualmente, podemos afirmar, que no previsto no artigo 17.º da LC, ou seja, a apreensão de correio eletrónico e registos de comunicação de natureza semelhante, a sua equiparação com o previsto no artigo 179.º do CPP, à interceção de comunicações e registo de transmissões de dados informáticos é aplicado, com as devidas alterações e adaptações, o regime da interceção e gravação de conversações ou comunicações telefónicas dos artigos 187.º, 188.º e 190.º, todos do CPP.

O artigo 19.º da LC consagra o recurso às ações encobertas e remete para a Lei n.º 101/2001, de 25 de agosto, que nos apresenta o regime e as regras deste tipo de ações. Sem estarmos a alongar-nos sobre esta temática, que será discutida mais à frente nesta dissertação, podemos referir que as ações encobertas podem ser admitidas em situações de crimes previstos na LC e os cometidos por meio de um sistema informático, que tenham uma cuja moldura penal máxima abstrata, seja, superior a 5 anos, e no caso de pena inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual de menores ou incapazes, a burla qualificada, a

[46] Fernando Gonçalves e Manuel João Alves, "A prova do crime – meios legais para a sua obtenção" (Coimbra: Almedina, 2009), páginas 230 e seguintes.

burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras e ainda os crimes previstos no título IV do CDADC.

3. Capitulo II

Malware

3.1. Tipos de *malware*

Malware pode ser definido como um conjunto de instruções que corre em certo sistema informático e faz com que este produza algo que o atacante queira. Na introdução desta dissertação, já aludimos, que o *malware* pode tomar variadas formas e configurações. Dito isto, este tipo de *software* é conhecido, digamos, como um contaminante dos sistemas informáticos, além de que é muitas vezes camuflado ou/e encaixado dentro de arquivos e códigos considerados não maliciosos. Além disso, em alguns casos, o *malware* apenas vai executar um conjunto limitado de tarefas, sendo que não terá qualquer interação com o atacante após a infeção. Já noutros casos, e de forma mais preocupante, o *malware* conterá uma "porta de trás", ou seja, algum programa que vai permitir aos invasores conseguirem passar pelos controles de segurança normais de um sistema informático e assim terem acesso ao todo do sistema comprometido.[47]

O *malware* pode ser dividido em variados tipos, sendo o critério de divisão o método de operação do *software* em causa. Podemos aqui, como exemplo, apresentar três tipos de *malware*, tendo em conta as características que destes advêm.

Em primeiro lugar, surge-nos o *malware* autorreplicante (*self-reflicating malware*), este caracteriza-se por criar novas cópias, ou instâncias, por si só, de forma a tentar ativamente propagar-se. Além disso, este tipo de *malware* pode ser propagado de forma passiva por um utilizador, no momento em que este o copia acidentalmente. Deste tipo de *malware* podemos elencar, como exemplo, o vírus.

Em segundo lugar, encontramos o *malware* parasítico (*parasitic malware*), este necessita sempre de um outro código executável para poder existir. Assim, o *worm* é o principal modelo, deste tipo de *software*, sendo conhecido publicamente como uma epidemia global. Além disso, integra neste contexto, a expressão "executável", que deve ser tida de uma forma muito ampla, para que se possa incluir tudo que possa ser executado. A título de exemplo, o código de bloco de inicialização num disco ou o código binário. Cabe-nos, referir ainda, que pelo facto de ser

[47] Christodorescu Somesh, et al., "*A semantics-based approach to Malware Detection*", (University of Wisconsin, USA, 2007), página 62 e ss..

autorreplicante, não necessita de interação humana para se propagar, tal como acontece com o primeiro tipo de *malware*.

Por último, encontramos o exemplo do Cavalo de Tróia, como um tipo de *software* malicioso, que aparentemente tem um uso benigno para o utilizador do sistema informático, mas tem escondida uma função maliciosa, ou seja, em primeira análise o *software* promete uma coisa, todavia, em segundo plano transmite algo diferente do que aparenta.

Hoje em dia, o *malware* é usado por variadas razões e em diversas situações, sendo que a mais preocupante, é a utilização por parte de *black hat hackers,* que muitas vezes, hackeiam instituições estaduais e governos, para roubar informações, por exemplo financeiras ou militares.

Como principais tipos de *malware* podemos apresentar o Vírus, o *Worm*, o Cavalo de Tróia ou *Trojan*, o *Logic Bomb*, o *Keylogger*, o *Screenlogger*, o *Spyware*, o *Adware*, o *Backdoor*, o *Exploits*, o *Sniffers* e os *Zombies*.

3.1.1. Vírus

Em primeiro lugar podemos encontrar o Vírus.[48] A forma deste se propagar é infetando cópias de si mesmo, tornando-se parte de outros programas e arquivos de um sistema informático. Tradicionalmente, os vírus propagam-se num único sistema informático, podem, ainda, "viajar" de um sistema informático para outro, quando são transportados pelos utilizadores destes, por exemplo num CD-ROM ou unidade *flash* USB.

Esta autorreplicação em código executável, existente é assim a característica chave deste tipo de *malware*. Além disso, ser difícil de detetar, ser inovador e ter capacidade de adaptação, são qualidades que também podemos atribuir aos vírus de sistema informático.

O vírus para funcionar e se tornar uma infeção no sistema informático, está dependente da execução dos arquivos hospedeiros e, assim, continuar o processo de infeção. Tem como intenção principal, tal como o nome indica, criar uma "virose" no sistema informático e assim infecioná-lo, de forma a destruir ficheiros ou conseguir aceder a certos ficheiros ou documentos do sistema informático.

Os vírus[49] podem ser distinguidos em variados tipos, para isso apresentamos algumas classificações de forma a clarificar o conceito de vírus:[50]

---

[49] As distinções, que faremos, de seguida, podem repetir-se para a maioria dos outros tipos de *malware*.

[50] Michael Davis, Sean Bodmer e Aaron Lemasters, "*Hacking Exposed – Malware & Rootkits: Malware & Rootkits & Secret Solutions*", (EUA: McGraw-Hill, 2010).

- A primeira que podemos apresentar, é a forma de classificar os vírus por o que eles pretendem atingir, sendo que neste caso, dividimos os vírus em três tipologias, os que infetam o setor de inicialização, os que infetam os arquivos executáveis e por ultimo os que infetam os arquivos de dados.

Um vírus do setor de inicialização é um vírus que se vai propagar autorreplicando-se no bloco de inicialização do sistema informático. Primeiramente, vai copiar o conteúdo do antigo bloco de inicialização do disco, para que mais tarde, possa transferir o controlo para o vírus, e assim, conseguir completar o processo de inicialização. Um dos maiores problemas com a utilização deste tipo de vírus, é que salvar o bloco de inicialização de um sistema informático requer muitas linhas de código, sendo que é necessário um método alternativo, ou seja, é quase sempre necessário copiar o bloco de inicialização original, num local fixo e "seguro" dentro do disco. Em geral, infetar o setor de inicialização é estrategicamente viável, visto que, e apesar, do vírus poder estar num local conhecido, vai estabelecer-se antes de qualquer *software* antivírus iniciar ou a segurança do sistema operativo estar habilitada, logo poderá propagar-se com mais facilidade e sem grandes entraves.

Seguidamente, encontramos os vírus de arquivos. Este tipo de vírus vai infetar arquivos que o sistema operativo do sistema informático considera executável, sendo que os executáveis binários são o alvo mais comum deste. No tipo de vírus descrito no parágrafo anterior, este vai ser inserido no bloco de inicialização, e assim, é executado através da sequência de inicialização normal de um sistema informático. Por outro lado, os vírus de arquivo possuem mais algumas opções à disposição, podendo inserir-se no início do arquivo, ou no fim do arquivo. Neste caso, um vírus que se coloca no início do arquivo, obtém o controlo desde o primeiro momento em que o arquivo é executado, chama-se a isto vírus de pré-carregamento. Em contraste, o vírus que se coloca no final de um arquivo é chamado de vírus adicional, sendo que a aplicação deste vírus é bem mais fácil que a do anterior.

Existem algumas formas para este tipo de vírus ter controlo sobre o sistema informático e assim conseguir propagar *malware*. A primeira define-se por as instruções originais no código poderem ser salvas e substituídas pelo código malicioso. Mais tarde, o vírus transferirá o controlo do sistema informático para o código infetado. Estamos aqui perante duas opções. Neste caso, o vírus pode executar as instruções originais diretamente no local onde se encontra (fora do sistema informático), ou então o vírus pode restaurar o código infetado, de volta ao seu estado original e executá-lo.

Na segunda maneira, o vírus pode procurar e substituir seções de valores repetidos, na esperança de evitar danos ao código original, ou por outro lado o vírus poderá substituir uma qualquer parte arbitrária do arquivo comprometido, ou seja, um arquivo de dados com uma aparência inocente, pode ser usado para esconder o conteúdo original.

Na terceira forma, os atacantes conseguem a propagação dos vírus, comprimindo uma parte do código original para criar espaço para, o vírus, em si próprio, e descomprimir o código original quando o vírus tiver concluído a sua execução.

Outra forma que podemos aqui referir, é a possibilidade de um vírus se inserir no código de destino, movendo o código alvo para fora do caminho, intercalando pequenos fragmentos de código de vírus com o código de destino. Por outro lado, o vírus pode não se inserir dentro do arquivo, ou seja, é um vírus complementar, que vai se hospedar, de tal forma, que é executado naturalmente antes do código original. Consequentemente o vírus nunca modifica o código infetado e ganha controle, aproveitando o processo, pelo qual, o sistema operativo procura arquivos executáveis. Embora isso tenha as características de um Cavalo de Tróia, um vírus complementar[51] é um vírus "real", em virtude da sua caraterística de autorreplicação.

Por fim, na classificação dos vírus pelo alvo que estes atingem, encontramos os vírus de macro. Algumas aplicações permitem que os arquivos de dados tenham "macros[52]" embutidas. Assim, os vírus de macro podem ser considerados, devido às suas caraterísticas, vírus de arquivos de dados, mas como a sua forma predominante tem sido macros, consideramos importante fazer esta distinção.

Uma vez instalado nas macros globais, o vírus pode infetar todos os documentos que venham a ser editados no futuro. Do ponto de vista técnico, as linguagens de macro são de mais fácil utilização do que as linguagens de programação de nível inferior, sendo que este tipo de vírus é mais recorrente, devido à simplicidade em o codificar.

- Como segundo grande grupo de tipos de classificação dos vírus, elencamos a estratégia de ocultação que estes usam, ou seja a forma como se tentam esconder, tanto dos utilizadores, quanto dos *software* antivírus.

Começamos, pois, com este grupo, que apresenta, uma estratégia um pouco incoerente. Assim, o tipo de vírus que não usa a dissimulação para se tentar esconder, sendo que esta é uma

[51] Vírus completares são vírus que se colocam anteriormente no caminho da pesquisa com o mesmo nome que o arquivo de destino, sendo que assim este será executado primeiro.

[52] Macros são breves fragmentos de código escritos em um idioma que normalmente é interpretado pelo aplicativo, um idioma que fornece funcionalidade suficiente para escrever um vírus.

estratégia de ocultação que é notavelmente fácil de implementar num vírus de sistema informático. Escusado será dizer, no entanto, que não é muito eficaz, visto que, uma vez que a presença de um vírus é conhecida, é corriqueiro detetar e analisar este.

A segunda forma que podemos listar é a criptografia. Usar um vírus cifrado, a ideia é que o corpo do vírus[53] seja cifrada de tal maneira, que dificulta a sua deteção por parte de outrem, que não seja o atacante. Na verdade não podemos dizer que esta técnica se trata de uma aplicação de criptografia, mas sim de uma técnica de ofuscação. É necessário, um *loop decryptor* para se poder decifrar o corpo do vírus, e logo transmitir o controlo do sistema informático para o vírus, e subsequentemente, para o atacante. O princípio geral é que o *loop decryptor* é pequeno em comparação com o corpo do vírus e fornece um perfil menor para o *software* antivírus para detetar.

Em terceiro lugar, encontramos os chamados vírus furtivos, sendo que estes são um tipo de vírus que toma ativamente medidas para conseguir esconder a sua própria infeção e não apenas o corpo do vírus. Além de que tenta esconder-se de tudo e não apenas de antivírus. Um exemplo, das técnicas empregadas por estes vírus, para se esconderem de tudo e todos é: o carimbo de data / hora original de um arquivo infetado ser restaurado após a infeção, de modo a que o arquivo não pareça que foi alterado recentemente.

Alguns sistemas armazenam o carregador de inicialização secundário como blocos de disco consecutivos, para assim se simplificar a tarefa do carregador de inicialização principal. Nesses sistemas, há duas visualizações do carregador de inicialização secundário, como uma sequência de blocos e como um arquivo no sistema de arquivos. Um vírus deste tipo pode inserir-se nos blocos do carregador de inicialização secundário, deslocando os blocos originais para outro lugar do sistema de arquivos. O resultado final é que a visão usual do sistema de arquivos não mostra mudanças óbvias, mas o vírus está escondido e é executado com a cortesia do carregador de inicialização principal real.

As técnicas empregadas por este tipo de vírus, sobrepõem-se com às técnicas utilizadas pelos *rootkits*, sendo que estes eram, inicialmente, *kits* de ferramentas para pessoas que haviam entrado nos sistemas informáticos. Eles usaram esses *kits* de ferramentas para ocultar as suas faixas e evitar a deteção. Hoje em dia, os *rootkits* são usados como um *malware* independente.

Outro tipo de vírus que encontramos, dentro desta classificação é o oligomorfismo. Um vírus oligomórfico, é um vírus cifrado que se carateriza por possuir um pequeno número finito de diferentes *loops* de descodificador à sua disposição. O vírus, assim, vai selecionar um novo *loop*

[53] O corpo do vírus é composto pela infeção, pelo gatilho e pela carga útil.

descodificador para cada nova infeção. O *software* antivírus explorará este facto para conseguir detetar o vírus em causa, de modo que é logicamente necessário mudar o código do *loop* do descodificador a cada infeção. Em termos de deteção, o oligomorfismo só se torna um vírus marginalmente difícil de detetar, após a chave de vírus encriptada ser alterada aleatoriamente com cada nova introdução e, a única parte imutável do vírus, ser o código do descodificador, porque o *software* antivírus, em vez de procurar pelo código *loop*, ou seja a encriptação, vai procurar o vírus em si.[54]

Quase de mão dada com o tipo de vírus que apresentámos no parágrafo anterior, encontramos o vírus polimórfico, que tal como o vírus oligomórfico é um dos vírus cifrados, ou seja, ambos alteram o *loop* do descodificador a cada infeção. No entanto, um vírus polimórfico tem, para todos os efeitos práticos, um número infinito de variações de *loop* descodificador, sendo esta a principal diferença entre os dois. A ideia de ser infinito, ou seja, de possuir um número infinito de variações, leva a que o mecanismo de deteção da infeção deva ser independente do código exato utilizado pelo vírus.

O código de um vírus polimórfico é transformado a cada nova infeção, usando para isso um mecanismo de mutação. O resultado é um mecanismo que é extensível e que permite permutar código de diversas maneiras.

O penúltimo tipo de vírus, baseando-se na estratégia que usam para se ocultarem é o metamorfismo. Estes são os vírus que podemos considerar como polimórficos no corpo do vírus. Não são codificados e, portanto, não precisam do chamado *loop* descodificador, porque evitam a deteção por mudança, ou seja, uma nova versão do corpo de vírus é produzida para cada nova infeção. As técnicas de modificação de código usadas pelos vírus polimórficos vão aplicar-se também aos vírus metamórficos. Ambos empregam um mecanismo de mutação, exceto que no caso do vírus polimórfico não é necessário mudar o seu motor a cada infeção, pois este pode residir na parte criptografada do vírus. Em contraste, um mecanismo de mutação do vírus metamórfico tem que se transformar novamente a cada infeção. O metamorfismo é relativamente simples de implementar num vírus, que se espalha no formulário de código fonte, como vírus de macro. Um vírus também pode contar com ferramentas do sistema para o metamorfismo.

Por último, cabe-nos referir a criptografia forte. O principal problema deste tipo de vírus é que carrega as suas chaves para desencriptar consigo e, assim, é mais fácil serem descobertos por um *software* antivírus. Tal, pode parecer uma fraqueza necessária, porque para não serem

[54] John Aycock, "*Computer...*", página 38.

detetados pelos antivírus, deveriam não possuir as chaves em questão e se, um vírus não tem a chave, não pode desencriptar-se e executar o seu código.

Deparamo-nos, porém, com duas outras possibilidades. A primeira é aquela na qual a chave vem de fora para dentro, de um sistema infetado para o sistema informático em questão. Assim, um vírus pode recuperar a chave de um *site*, carregando a chave deste com ele, o que poderá levar ao bloqueio como uma contramedida. Para evitar saber o nome de um *site* específico, um vírus pode usar um mecanismo de busca na web para obter a chave e assim evitar ter de carregar a chave. Na segunda possibilidade, ao contrário da primeira a chave, vem de dentro de um sistema infetado. Usando a geração de chave ambiental, a chave de desencriptação é construída usando os elementos já presentes no ambiente do alvo, como o nome de domínio da máquina, a hora ou a data e alguns dados no sistema (por exemplo, conteúdo do arquivo).

3.1.2. *Worm*

O *worm* é outro tipo de *malware*,[55] que é capaz de se difundir automaticamente através de redes, remetendo cópias de si mesmo, de sistema informático para sistema informático. O *worm* apesar de ter variadas características e iguais, diferencia-se do vírus, na medida em que não embute cópias de si mesmo noutros programas ou arquivos, além de que não requer a sua execução para se poder propagar, ou seja, não necessita de nenhum código executável para se propagar, sendo independente. A sua propagação dá-se através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em sistema informático.

Os ataques que ocorrem são, quanto mais recente a variante do worm, mais sofisticados e fluídos nos métodos de propagação, que vão tornar-se na rede. Podemos estar perante um *worm* de contágio, que é comparado com uma "tempestade perfeita". Em termos de ser um *worm* que tem a habilidade de pular do servidor para os clientes de forma tão rápida e tão perfeita, que poderá infetar um número bastante absurdo de sistema informáticos com facilidade, num prazo de horas, mas atenção, apenas, quando executado corretamente.

Um dos primeiros *worms* utilizados nos experimentos do XCXXP no início dos anos 1980 não tinha como finalidade um objetivo malicioso. Pretendia-se com uma estrutura para a computação distribuída, usar o tempo de CPU que de outra forma não seria utilizado. Assim, um utilizador escreveu um programa para ser executado em paralelo, em diversas máquinas e ao mesmo tempo - este programa faria com que o mecanismo dos *worms* administrasse a mecânica

[55] Michel Davis, et al., "*Hacking Exposed*...", página 46.

para fazer o programa funcionar nas diferentes máquinas. Um número limitado de segmentos foram iniciados, e todos os segmentos mantinham contato uns com os outros. Se o *worm* perdesse o contato com um segmento (por exemplo, alguém reiniciasse a máquina em que o segmento estava a funcionar), os outros segmentos iam buscar outra máquina para executar o segmento em questão. Os *worms* tinham assim mecanismos de segurança, evitando a desconfiança dos utilizadores sobre este tipo de *software*. Contudo, os pesquisadores do Xerox PARC concluíram que gerenciar o crescimento e a estabilidade dos *worms* era deveras difícil e este tipo de *software* teve que ser parado.

3.1.3. Cavalo de Tróia

Em terceiro lugar, referimos os *Trojan* (ou Cavalo de Tróia)[56], a principal forma que este ostenta é passar-se por um "presente", como por exemplo na forma de cartões virtuais, de álbum de fotos, de protetor de ecrã ou de jogos. Este tipo de *malware* além de executar as funções para às quais aparentemente foi projetado, vai também executar outras funções, que na maior parte das vezes, são maliciosas e sem o conhecimento do usuário, ou seja, um Cavalo de Tróia é um programa que tem como principal função cumprir uma tarefa benigna, mas, que secretamente vai executar uma tarefa maliciosa adicional.

3.1.4. Outros tipos de *malware*

Logic Bomb[57] é um tipo de *malware* que apresenta um código que consiste em duas partes. A primeira parte é o que se chama de *payload*, ou seja, uma ação que ainda vai ser realizada. A chamada carga útil pode ser qualquer coisa, mas normalmente apresenta uma conotação com um efeito malicioso. Já na segunda parte do código, encontramos uma espécie de gatilho, uma condição booleana que é avaliada e vai controlar quando a carga está a ser executada. Esta espécie de gatilho, é ativado conforme a imaginação do *hacker*, e esta ativação pode basear-se em condições locais como uma data ou um momento, como por exemplo, quando o utilizador efetuar o login ou também pode ser projetado para ser desligado remotamente. Assim, as “bombas lógicas” podem ser inseridas no código existente ou podem ser autónomas. Outra característica deste tipo de *malware*, é que normalmente é conciso e discreto, especialmente misturado em

[56] John Aycock, “Computer Viruses ...”, páginas 12 e seguintes.
[57] Jonathan Clough, “Principles of Cybercrime”, (Cambridge: Cambridge University Press, 2010), página 33.

milhões de linhas de código fonte, e apenas a mera ameaça deste pode servir facilmente para extorquir dinheiro a uma empresa.

Apresentamos agora o *Keylogger* e o *Screenlogger*. O primeiro captura e armazena as teclas digitadas no teclado pelo usuário do sistema informático. Habitualmente, a ativação é subordinada a uma ação prévia do utilizador, como por exemplo, depois de um acesso ao *e-commerce* ou *internet banking*, para captura de senhas bancárias ou números de cartões de crédito. O segundo, é uma forma avançada de *keylogger*, e é capaz de armazenar a posição do cursor e a imagem que é apresentada no monitor, nos momentos em que o rato é clicado.

O Spyware também está presente no catálogo de *software* malicioso.[58] Este tipo tem como principal objetivo a monotorização das atividades de um sistema informático e enviar as informações que daí advêm a terceiros. São um dos *softwares* que poderiam ser usados de forma legítima, mas comummente, são usados de forma dissimulada, não autorizada e maliciosa, ou seja como o nome indica, são uns verdadeiros espiões. Este *malware* pode chegar num sistema informático de duas maneiras diversas, a primeira é num pacote com outro *software* que o utilizador instala, a segunda forma é a baseada na exploração de falhas técnicas nos navegadores da Web.

É, pois, outro género de *malware* que pode estar ligado e às vezes embutido em programas fornecidos oficialmente pelas empresas, como por exemplo, por *download* a partir de sites, mas que tem incorporada a funcionalidade de rastreamento adicional de forma oculta, e que reúne estatísticas de *marketing*. Uma situação, que exemplifica a utilização deste *software*, que era disponibilizado por uma empresa e mais tarde, foi descrito como ilegítimo, é o *rootkit* da Sony, um *trojan* embutido em CDs vendidos pela Sony, que se instalava silenciosamente, sendo que depois ocultavam-se nos sistemas informáticos, com a principal intenção de evitar a cópia ilegal.

Adware foi projetado para apresentar propagandas, sendo esta a sua principal função. Este tipo de *malware* é comum de aparecer quando se instala um programa no sistema informático. Tem semelhanças com o *spyware*, visto que, ambos se concentram em reunir informações sobre o utilizador e os seus hábitos. O *adware*, ao contrário do *spyware*, tem o foco mais virado para o *marketing* e a publicidade, e pode fazer aparecer anúncios ou redirecionar o navegador do utilizador para determinados sites, com o único fim de efetuar uma venda. O *adware* também pode recolher e transmitir informações sobre os usuários que vão ser usadas mais tarde

[58] Jonathan Clough, "*Principles of Cybercrime*", página 36.

para fins de *marketing*. Tal como acontece com o *spyware*, o *adware* não tem a possibilidade de se auto-replicar.

Apresentamos agora o tipo de *malware* que possibilita a um invasor retornar a um sistema informático que já foi comprometido, assim estamos perante um mecanismo que ignora as verificações de segurança, consideradas normais num sistema informático. Certos programadores criam por vezes as chamadas, portas traseiras por motivos legítimos, como ignorar um processo de autenticação demorado ao depurar um servidor de rede. Tal como verificamos que acontece com as "bombas lógicas", este tipo de *software* maligno pode ser colocado num código legítimo de forma a não ser notado ou então pode ser autónomo, é portanto vulgarmente conhecido por "porta dos fundos", ou seja, estamos perante o *Backdoor*.

O próximo tipo de *malware* foi projetado de forma a poder explorar uma vulnerabilidade que já existe num *software* de sistema informático, sendo este o *exploits*.

O *sniffers* tem como principal utilidade a possibilidade de ser usado para capturar e armazenar dados trafegando numa rede de sistemas informáticos. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam a ser empregadas conexões sem recurso à criptografia.

O *malware* que dá pelo nome de *Port Scanners* serve para efetuar "varredelas" nas redes de sistemas informáticos, tendo como intuito identificar quais os sistemas informáticos que estão ativos e quais os serviços que estão sendo disponibilizados por eles. Este tipo de *software* é amplamente utilizado pelos atacantes para poderem identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados num sistema informático.

O *bot* além de incluir funcionalidades de *worms*, dispõe de mecanismos de comunicação com o invasor, permitindo, assim, que o programa seja controlado remotamente. O invasor, ao comunicar-se com o *bot*, pode orientá-lo, de forma a desferir ataques contra outros sistemas informáticos, como por exemplo furtar dados e também enviar *spam*.

O Rootkit é um conjunto de programas que tem como principal fim o de esconder e assegurar a presença de um invasor num sistema informático que já se encontra comprometido. Apesar de ter como nome "*rootkit*", este não é empregado para obter acesso privilegiado (*root* ou administrador) a um sistema informático a funcionar normalmente e que não foi submetido a nenhum *software* malicioso, mas sim para manter o acesso privilegiado num sistema informático que já foi previamente comprometido.

Os sistemas informáticos que se encontram comprometidos podem vir a ser usados pelos *hackers* para um sem fim de tarefas, sem o utilizador legítimo de tal sistema se aperceber. Assim sendo, os sistemas informáticos usados pelos atacantes desta maneira são chamados de *zombies*. Este tipo de *malware* carateriza-se por ter como principal função, fazer com que os sistemas informáticos infetados enviem *spam* e participem em ataques de negação de serviço, que são coordenados em grande escala. O uso deste tipo de *software* malicioso, prende-se com o facto do envio de *spam* violar os bons costumes e a moral do uso da internet, para não aludir, que em alguns casos pode violar. Por conseguinte, os *spammers* enviam *spam* destes sistemas informáticos comprometidos, de tal forma que não possam vir a ser descobertos, sendo portanto, um recurso livre e descartável.

Por último, apresentamos o *Quantum*, este tipo de *malware* cria um *site* falso para depois poder implantar sistemas, é usado pelo GCHQ na Vigilância de Sistema informáticos e Redes. É caraterizado, por ser um método de implantação de *malware*, através de redireccionamento para *sites*, que exploram, via *web*, vulnerabilidades dos sistemas informáticos das vítimas.

3.2. Formas de instalação de *malware* e o seu funcionamento

Neste subcapítulo, analisaremos os métodos, pelos quais, o *malware* consegue "entrar" nos sistemas informáticos em risco de serem comprometidos. Existe uma panóplia de formas ativas de enviar ou entregar *softwares* maliciosos à pseudovítima. Além disso, existem, também, métodos de infeção passiva, que estão dependentes da engenharia social ou do acesso, por parte da futura vítima, ao conteúdo, onde o *malware* se encontra armazenado.

Os sistemas informáticos podem ser infetados com programas de Cavalo de Tróia e outros tipos de *malware* de variadas maneiras.

Assim, elencamos, como métodos de propagação de *malware:*

- A utilização de correio eletrónico, ou seja, via *e-mail;*

- O uso de páginas *web*, tal como os *downloads* quando se visita determinada página *web*;

- O *phishing* seja ele passivo ou ativo;

- A exploração de serviços de rede, a junção de *software* maligno com outro tipo de *software* considerado benigno.

A maioria das formas de comunicação digital tem a capacidade de transmitir, todo o tipo de *malware*, sendo que depois, podem vir a descarregar arquivos ou a alterar dados. Muitos dos

métodos de propagação de *software* malicioso requerem intervenção dos utilizadores do sistema informático, mesmo que seja um simples clique no teclado. Ainda que consigamos verificar a propagação de, por exemplo, os vírus que advêm do correio eletrónico, há sempre a possibilidade de os utilizadores serem enganados e por isso, abrirem arquivos desconhecidos ou ainda quando os usuários de certa rede informática fazem *download* de um *software* gratuito e considerado útil, sem grande cautela. Os atacantes podem usar, por exemplo, programas de Cavalo de Tróia, vírus e outros tipos de *malware* para assumir o controlo do sistema informático, de um utilizador imprudente.

O primeiro método que vamos referir no que diz respeito à propagação de *malware* é, também, um dos mais utilizados no dia-a-dia: o correio eletrónico.[59]

Ao longo dos últimos dez anos, o *e-mail* foi tido como a falha dos administradores de rede, sendo, podemos afirmar um tipo de portal aberto para todos os que desejam invadir as redes alheias e assim aceder ilegitimamente a um sistema informático.[60] Esta foi a realidade, absoluta, na década de 90 e hoje em dia, continua a ser, um dos meios de propagação de *software* malicioso mais comummente utilizado. O *e-mail* é uma das duas formas consideradas, sempre abertas, nas redes informáticas, sendo a segunda os sites maliciosos. Os usuários/clientes são os principais agentes deste tipo de propagação, sendo que, para que esta se dê, é necessário que o indivíduo aceder e abrir o *e-mail*.

As técnicas de injeção de *malware,* em forma de um *e-mail*, contêm uma vertente onde se explora o lado pessoal do indivíduo. A engenharia social é, portanto, uma base fundamental para a maior parte (sem irmos mais longe e dizermos todos) destes ataques. Uma forma de evitar, hoje em dia, é verificar os *links* dos *e-mails*, a sua origem, que na maioria das vezes executam uma explicação do lado do utilizador quando são clicados.

Podemos ainda referenciar uma técnica de utilização do correio eletrónico como meio de propagação de *malware*, eficaz e inteligente, conseguindo descarregar a sua própria biblioteca dinâmica de comunicação segura (ssl.dll)[61], que vai habilitar o *malware* a abrir um canal secreto próprio, ou seja, escondido nos sistemas externos de *e-mail* (tais como, a *yahoo*, o *hotmail*, o *gmail*). Isto quer dizer, que as comunicações dentro de certas redes privadas, que se dirigem aos sistemas públicos de *e-mails* pessoais, são como um login para o *malware*, permitindo a este,

[59] Jonathan Clough, "*Principles of Cybercrime*", página 32.
[60] Michael Davis, et al., "*Hacking Exposed…*", página 31.
[61] *Secure Socket Layer Dynamic Link Libraries*.

receber novas atualizações ou/e instruções ou/e dados, que podem estar a ser partilhados dentro da rede interna.

Como segundo método de propagação de *malware,* podemos referir as páginas maliciosas na internet. Qualquer *site* pode ser mal-intencionado, e mesmo estando perante um *site* fidedigno, este pode ficar "preso" a entidades mal-intencionadas que carregam o *malware* no próprio *site*, na expectativa assim os utilizadores deste, que desconhecem a verdadeira intenção por detrás de toda a página *web*, a visitem e, imediatamente, vejam os seus sistemas informáticos ou a rede em que eles se inserem contaminados com *software* malicioso. A título de exemplo e mera curiosidade, segundo Kaminsky[62] hoje em dia, podemos encontrar 1 em cada 5 páginas *web* que estão em risco de serem infetadas por *malware* e, assim, se tornarem em *sites* com conteúdo malicioso.

A base que está por trás dos ataques que se, efetuam em certos *sites* é a exploração feita ao lado do utilizador/cliente. É tão simples que quando se visita uma certa página *web* e baixa-se o código desta, o *malware*, é executado localmente e escondido nos pacotes da sessão HTTP, normalmente incorporado nestas, de maneira a ficar encoberto, sendo que os *firewalls*, *NIDS* e antivírus não conseguem verificar a presença de um *software* malicioso. É essencial que os usuários entendam que navegar na internet pode trazer *malware* para os seus sistemas informáticos ou redes informáticas.

Interligada com este tipo de propagação de *malware* encontramos as redes sem fio. Frequentemente, estas aos milhares, se não milhões, que estão conectadas à Internet, muitas vezes, com pouca ou nenhuma segurança habilitada, tornam-se, portanto, um meio bastante apetecível para os *hackers* e invasores, poderem conseguir aceder a um sistema informático, utilizando as redes sem fio, para propagar os *softwares* maliciosos.

O *phishing*[63] é, atualmente, mais uma das formas com que os usuários dos sistemas informáticos e, consequentemente, da web tem de se preocupar, visto que é, um meio de propagação de *malware*. Podemos caracterizar o *phishing* como uma fachada inteligente, utilizada por parte de certos *hackers*, para atrair os utilizadores a clicar em certo *link* ou fornecer informações pessoais ou profissionais, que possam divulgar detalhes suficientes, que, mais tarde, vão permitir que o invasor tenha a possibilidade de roubar a identidade dessa pessoa ou obter mais informações profissionais, ou mesmo pessoais sobre o sujeito em si, a fim de obter acesso

[62] Michael Davis, et al., "*Hacking Exposed*...", página 36.
[63] Michael Davis, et al., "*Hacking Exposed*...", página 40 e ss..

a um recurso de informação privado ou público e, podendo, causar danos ou obter lucro. Resumindo, a pessoa recebe um e-*mail* e este não passa de um meio para propagar algum tipo de *malware*.

Um *hacker* pode enviar mais de 1.000.000 *e-mails* de *phishing*, e basta, apenas, que um por cento dos destinatários (um número que parece irrisório) abra esse *e-mail*, e assim terão a sua identidade, possivelmente, roubada ou o seu sistema potencialmente controlado pelo hacker, que o *phishing* fornece resultados, para o lado dos que tentaram infiltrar *malware* nos sistemas informáticos das 1.000.000 pessoas. Na maior parte das vezes, este tipo de propagação é feita com uma lista internacional de destinatários, de forma a garantir que as entidades internacionais que cooperam legalmente, tenham variadas dificuldades em conseguir coordenar qualquer tipo de apreensão dos operadores de *malware*.

A propagação de *malware* de *e-mail* é considerado o método de *phishing* mais efetivo e eficiente, muitas vezes utilizando o *spam*. No entanto, o *spear-phishing* voltou a aparecer nos últimos anos.

As principais ameaças provenientes do *phishing* são a perda de informações pessoais e das informações das empresas (um dos alvo bastante utilizados neste método) que podem ser extraídas das redes informáticas. Exemplo concreto, às vezes, é o simples gesto de clicar nos botões de um *site* mal-intencionado, dando-se, assim, a aprovação que o sistema informático precisa, para começar a carregar o *malware* em segundo plano, enquanto o utilizador está a preencher um formulário, ou a aguardar o processo de envio final. De salientar, que o *phishing*, está conotado com técnicas que visam a obtenção de informações, consideradas, privadas da vítima.

Existem dois tipos principais de ataques de *phishing*, os passivos e os ativos. Em primeiro lugar, falaremos do *phishing* ativo. Este é caraterizado por esquemas baseados em correio eletrónico e, onde normalmente, se solicita ao utilizador da rede que, faça um clique sobre algum *link*, enquanto está a ler o correio eletrónico. Assim o utilizador irá ser encaminhado para uma página *web* falsa, sendo que esta é muito semelhante à página *web* real. Maioritariamente este tipo de esquemas, de *phishing* ativo, são configurados para atacar empresas, visto que o utilizador da rede informática de certa empresa, alvo deste método de propagação de *malware*, confia nas páginas *web* que utiliza, porque aparentemente fazem parte do *software* cedido pela empresa ou porque terá uma conta numa destas páginas que será usada para criar as falsas.

O *phishing* ativo também pode ser visto em anúncios gratuitos. Neste caso o utilizador recebe um *e-mail* oferecendo, por exemplo "um certificado de 500 € gratuito", caso ele se disponibilizasse a preencher um formulário, enviar a informação e, possivelmente, fornecer os endereços de *e-mail* de vários amigos.

Seguidamente trataremos das características e consequências encontradas no *phishing* passivo. Neste caso os esquemas para a propagação de *malware*, são geralmente inseridos em páginas *web* inativas, que estão ligados a consultas do mecanismo de pesquisa. Os utilizadores são, digamos, aliciados com um formulário onde lhes é pedido para preenchê-lo com dados pessoais e depois enviá-lo. A maior parte das vezes, quando, os utilizadores enviam o formulário, a página *web* recarrega outra vez de forma igual, levando a uma frustração por parte do utilizador que vai acabar por sair do *site*. Este tipo de abordagem passiva tem assim dois resultados. O primeiro é que a informação fornecida é usada com outra finalidade, porém, de forma maliciosa. Já no segundo, o *site* executa logo o *malware*, após o utilizador carregar no botão de envia-lo e, sendo que em seguida, se dá a propagação do *software* malicioso no sistema informático.

Mais uma das formas de propagação de *malware* é a possibilidade que os atacantes tem, em explorar as vulnerabilidades na segurança dos sistema informáticos dos utilizadores, sendo que aproveitam qualquer brecha, para conseguirem correr qualquer tipo de programas à sua escolha, nos sistemas informáticos e nas redes informáticas, através da mais pequena falha de segurança.

Consideramos importante, referir ainda o caso dos *worms*. Estes encontram cinco estratégias para poderem-se propagar. A primeira é o *scan* aleatório, aqui podem selecionar um alvo escolhendo, aleatoriamente, um valor para usar como um endereço IP. Isso foi feito, por exemplo, por Código Vermelho I.

A segunda estratégia que encontramos é o *scan* localizado. Enquanto a primeira estratégia é boa para uma distribuição generalizada, mas é uma abordagem de sucesso para *worms* que exploram vulnerabilidades técnicas para se propagarem. É muito mais provável que os sistemas informáticos que se encontrem na mesma rede informática, sejam mantidos da mesma forma. Assim, o *scan* localizado tenta tirar partido disto. As máquinas alvo são, novamente, escolhidas aleatoriamente, mas com uma inclinação para máquinas locais. Uma "máquina local" é selecionada heuristicamente, aproveitando o compartilhamento do endereço IP descrito acima. Por exemplo: o Código Vermelho II escolheu os endereços IP alvo, dessa maneira.

A terceira estratégia que apresentamos é a verificação da lista de ocorrências, ou seja, antes do *worm* ser inserido no sistema informático, pode ser compilado um "*hit-list*" que contém os endereços IP de algumas máquinas, conhecidas como vulneráveis a uma falha técnica que os planos de *worm* exploram. A lista não precisa ser 100% precisa, uma vez que só será usada como ponto de partida. Não precisa conter um grande número de endereços IP - são suficientes 50.000 ou menos. Após a sua libertação, o *worm* começa com a segmentação das máquinas mencionadas na lista de ocorrências. Cada vez a propagação se dá com sucesso, ele divide o restante da lista ao meio. Quando a lista está esgotada, o *worm* pode voltar para outras estratégias de *scan*.

Referimos agora a quarta estratégia, de propagação dos *worms*. Sendo esta o *scan* da permutação. Este tipo de *scan* caracteriza-se pelo facto de haver um compartilhamento do espaço de um enderenço IP, ou seja, caso a máquina já esteja infetada, o *worm* faz com que as instâncias da máquina sejam compartilhadas numa permuta comum do espaço de endereço IP. Cada nova instância recebe uma posição na sequência, para começar a infetar. O *worm* continua a funcionar através dessa sequência. Se uma máquina é encontrada e já está infetada, o *worm* escolhe um novo ponto na sequência aleatoriamente, dando a este, um mecanismo simples, para a coordenação distribuída sem qualquer sobrecarga de comunicação entre instâncias de *worm*.

Deparamo-nos agora com o *scan* topológico, como mais um tipo de estratégia usada pelos *worms* para se poderem propagar nos sistemas informáticos. É chamado de *scan* topológico, quando as informações sobre os sistemas informáticos infetados podem ser usadas para escolher novos destinos, em vez de se fazer uma pesquisa aleatória, como nos *scans* anteriormente expostos. Neste caso, o *worm* segue a topologia da informação que encontra. A topologia seguida pode ou não coincidir com a topologia da rede física. Um *worm* pode seguir informações sobre as interfaces de rede de uma máquina para novos alvos, mas outros tipos de informações podem resultar em propagação ao longo das redes sociais. O *scan* topológico é particularmente útil, no que toca a propagação em espaços de endereço grandes e dispersos. Em contraste, o *scans* aleatório desperdiça muitos alvos de localização de esforço, num espaço com essas dimensões.

Por último, apresentamos o *scan* passivo. Neste caso o *worm* pode aguardar que lhe cheguem informações topológicas. Um *worm* a fazer um *scans* passivo, pode espiar o tráfego de rede, para reunir informações sobre, por exemplo, endereços IP válidos, e sobre o sistema operativo e serviços de sistemas informáticos.

4. Capitulo III

Neste capítulo discutimos os chamados métodos ocultos de investigação e todos os problemas associados. Embora não constituam uma novidade no seio do processo penal, foi nas últimas décadas que se viu um incremento no seu uso. Englobam-se neste conceito as figuras do agente encoberto, infiltrado e provocador. Como traço comum, estas figuras caracterizam-se pela inserção de forças policiais, ou de terceiros com estas concertados, em ambientes criminosos como forma de obter provas que permitam a criminalização de um possível suspeito.

O desejo de uma justiça célere e rápida que satisfaça o protesto dos cidadãos, que se encontram em estado de pânico, perante os fenómenos da nova criminalidade, tais como, o crime organizado transnacional[64] e do terrorismo, e os crimes informáticos, foi uma das razões, que conduziu à implementação de meios de obtenção de prova especializados, especiais e excecionais.

Estes meios de obtenção de prova excecionais e por vezes ocultos são: a ampliação do âmbito das interceções telefónicas, registo de voz-off e imagem, gravações ambientais, gravações e fotografias por meio de câmaras de videovigilância, agentes infiltrados física e digitalmente, rastreios e persecuções digitais, localizações celulares, controlo e monitoramento concreto de IP, IMEI e GPS, buscas e apreensões preventivas no sistema digital a nível nacional, regional e internacional sem qualquer conhecimento do visado, e a admissibilidade e utilização como meios de prova os relatórios elaborados pelos serviços secretos.[65]

4.1 Requisitos para o uso dos métodos ocultos de investigação

Os métodos ocultos de investigação sacrificam, à passagem, um elenco de bens jurídicos ou/e direitos fundamentais tão sobressaídos como por exemplo: a privacidade, a intimidade, a palavra, a imagem, a inviolabilidade do domicílio, o sigilo das telecomunicações e a confidencialidade e integridade dos sistemas técnico-informacionais. Isto num plano material-substantivo. Já no que diz respeito ao plano estritamente adjetivo-processual, podemos elencar como exemplo dos direitos suscetíveis de serem violados por este tipo de métodos, o direito a recusar testemunho ou depoimento e, ainda, o direito ao silêncio.

[64] Crime de tráfico de armas, de droga, de seres humanos e de órgãos humanos.

[65] Manuel M. G. Valente Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias". Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 3, n. 2, p. 473-482, mai./ago. 2017.

Salientamos ainda, que estes meios de investigação têm uma tendência para invadir a esfera jurídica, de um número incontrolável de pessoas, não conhecendo em primeira mão, a diferença entre suspeito e inocente e não respeitando, à partida, as relações de segredo e de confiança. Além de que, as pessoas não têm conhecimento das ações que decorrem destes meios, antes e durante a sua execução, não podendo atualizar qualquer pretensão de reação e tutela, mesmo quando tem direito a tal.

Os métodos ocultos de investigação criminal, possíveis de violarem direitos e interesses legalmente consagrados, devem obedecer a um número de requisitos e condições, que vamos elencar nos próximos parágrafos[66].

Em primeiro lugar, encontramos a exigência que este tipo de meio apenas pode ser autorizado e legitimado, por uma Lei da Assembleia da República ou por um Decreto-Lei do Governo, mediante devida autorização pelo Parlamento.

Complementando a reserva da lei[67], encontramos mais um requisito, a obrigatoriedade da seleção de um catálogo de infrações criminais, ou seja, é necessário uma fragmentaridade de 1º grau, obtida através de um catálogo de crimes. Este tem, ele próprio, de responder a certas exigências, como, a adoção apenas de infrações, suficientemente gravosas, que legitimam o uso de métodos ocultos de investigação criminal e também, a adoção de critérios de proporcionalidade e de restrições das infrações, que vão legitimar a gravosa medida de ocultação de obtenção de prova.

Em concreto, e de forma a prevenir e a combater, estas novas formas de criminalidade, no âmbito material, o legislador e o intérprete têm alargado os espaços de recurso que de forma positiva em lei, aumentando o elenco de crimes que admitem o recurso aos meios excecionais de investigação.

Em segundo lugar, afirmamos que é necessário, haver uma suspeita fundada em factos concretos e medidos, através de critérios de plausibilidade ou probabilidade, para podermos dar uso a métodos ocultos de investigação criminal, ou seja, além de estarmos perante um crime do catálogo referido no parágrafo anterior, é necessário a verificação de uma suspeita de uma ocorrência dos crimes, previstos no elenco.

Em terceiro lugar, um dos requisitos indispensáveis para a utilização de métodos ocultos de investigação criminal, é a subsidiariedade ou princípio pela preferência dos métodos menos

[66] Benjamim Silva Rodrigues, "Direito Penal – Parte Especial...".

[67] Princípio da fragmentaridade caracteriza-se pelo facto de o direito apenas ocupar-se de uma parte dos bens jurídicos tutelados pelo ordenamento jurídico, deixando os outros bens jurídicos a outros ramos do direito, tais como as contraordenações.

lesivos, ou "abertos", de investigação criminal face aos ocultos. Assim, sempre que os métodos menos lesivos forem suficientes para se obter a prova necessária à descoberta da verdade material, deve preferir-se estes, em relação aos demais, mais lesivos e ocultos. Visto que estes produzem uma maior devassa dos interesses e direitos legalmente consagrados, são, claramente, mais nocivos os métodos ocultos de investigação criminal. Portanto fica proibida a possibilidade de lançar mão destes meios de investigação criminal, no caso dos métodos "abertos" serem eficientes e suficientes.

A subsidiariedade tem de se concretizar de três maneiras:

- A subsidiariedade para fora dos métodos ocultos de investigação;

- A subsidiariedade para dentro dos métodos ocultos de investigação e

- A subsidiariedade excludente da cumulação dos métodos ocultos de investigação.

Na primeira, dá-se preferência aos métodos "abertos", sempre que estes atinjam o objetivo de obtenção de prova, vedando-se o recurso a todos os métodos mais gravosos.[68]

Na segunda vertente, deve, dentro dos meios ocultos de investigação, haver uma real subsidiariedade, de tal modo que se vai proibir o recurso a um meio mais gravoso, quando um menos gravoso e igualmente idóneo, seja bastante, para a prossecução dos interesses da concreta investigação criminal. Por último, Costa Andrade,[69] afirma que a ideia de subsidiariedade provoca um efeito de exclusão ou proibição, de princípio da cumulação de vários métodos ocultos de investigação. Assim, só em *ultima ratio* se deve usar a cumulação deste tipo de métodos, e sempre em consonância com as exigências da proporcionalidade.

Outro dos critérios defendidos por Costa Andrade[70] e também por nós para a possibilidade da utilização de métodos ocultos de investigação criminal, é o princípio transversal da proporcionalidade *stricto sensu*. Quer no conjunto das infrações integrantes do catálogo, quer no grau ou fundamentação da suspeita ou ainda, de que na ideia de subsidiariedade está inscrita a ideia de proporcionalidade em sentido estrito, ou seja, a exigência de uma balança equilibrada, em que de um dos lados está a gravidade da intromissão e no outro está o peso das razões

[68] Podemos exemplificar com o art. 187.º do CPP introduzida pela reforma de 2007, que sujeita a utilização da escuta aos princípios da indispensabilidade da descoberta da verdade ou da impossibilidade ou de muita dificuldade de obter a prova por meio menos oneroso. É pacífico que existe uma graduação de meios a mobilizar pela ordem elencada pelo legislador, ficando os mais gravosos, dentro de eles os meios ocultos de investigação criminal, pela sua especial aptidão para afrontar direitos fundamentais, tais como, a reserva da intimidade da vida privada, inviolabilidade do domicílio e das telecomunicações e da correspondência, imagem, palavra e honra. Cabe, portanto, aos operadores judiciários a obrigação de provar a impossibilidade ou a dificuldade de proceder à investigação através de um meio menos oneroso para que se obtenha a prova. Manuel Monteiro Guedes Valente, "Escutas Telefónicas, Da excecionalidade à vulgaridade", 2ª Edição, (Coimbra: Almedina, 2008).

[69] Manuel da Costa Andrade, "Bruscamente no Verão Passado, a Reforma do Código de Processo Penal - Observações Críticas sobre uma Lei que Podia e Devia ter sido Diferente", (Coimbra: Coimbra Editora, 2009), página 58.

[70] Manuel da Costa Andrade, "Bruscamente no Verão Passado...".

investigatórias (como a descoberta da verdade) que justificam a utilização de certo tipo de método oculto de investigação.

Além desta proporcionalidade em sentido estrito, temos ainda de referir o princípio da continuidade ou atualidade dos métodos ocultos e respetiva proporcionalidade, ou seja, é necessária de todas as vezes que se recorra ao uso de um destes meios, fazer um levantamento de todos os métodos ocultos de investigação, e, de acordo com este, (tendo em conta critérios como a danosidade e a sua hierarquização), escolher o mais proporcional, relativamente ao caso em concreto.

O quinto requisito exigido para a utilização é a proibição absoluta de aniquilamento do "âmbito pessoal ou nuclear" da intimidade. Assim, é extremamente necessário com a utilização de métodos ocultos e investigação criminal, implementarem-se áreas de defesa ou de proibição da lesão do âmbito pessoal, ou área nuclear da intimidade e também de certos direitos processuais penais do arguido, tais como o direito à recusa de testemunhar e ao silêncio. Este requisito existe precisamente, para garantir a não violação de princípios e direitos constitucionalmente consagrados, tais como a dignidade da pessoa humana e o livre desenvolvimento da personalidade, além de defender direitos considerados processuais, como os referidos na frase anterior.

A reserva da lei é uma das formalidades exigidas para o uso de métodos ocultos de investigação criminal. Seguindo esta linha, outro dos requisitos necessários é a reserva do juiz de instrução. É a este que se impõe a possibilidade de autorizar o uso de métodos de investigação oculta. Sendo esta uma exigência orgânica-procedimental da judicialização da autorização da medida, pretende-se, com esta, evitar o uso da medida quando não é justificada a danosidade e assegurar uma tutela preventiva dos direitos de uma pessoa, exposta à invasão e à devassa sem qualquer possibilidade de assegurar a sua defesa, pois somente o juiz pode efetuar este controlo.

Por fim, um dos últimos requisitos para utilizar estes meios de investigação, e não é demais salientar que o elenco de requisitos necessários para esta utilização é extenso, pelo facto, de estarmos perante meios que violam direitos e interesses legalmente, e muitas vezes constitucionalmente, protegidos, é a exigência do princípio da atualidade da medida judicial autorizativa. Neste princípio fica deslegitimado o método oculto de investigação que seja levado a cabo após um enorme lapso de tempo sobre a autorização judicial, pois a necessidade da medida é aferida à luz dos conhecimentos que o juiz dispõe no momento em que emite a sua autorização. A autorização judicial deve pois, fixar uma duração máxima para o uso do método oculto de

investigação, tendo em conta sempre os critérios de proporcionalidade e de adequação necessários.

4.2. Tipos de métodos ocultos de investigação criminal

Na esfera jurídica portuguesa, podemos afirmar que existem variados tipos de métodos ocultos de investigação, são eles os que ocorrem dentro das redes e ou serviços de comunicações publicamente acessíveis. Outros, pelo contrário, ocorrem à margem ou fora de tais redes ou serviços. Encontramos, também, alguns métodos que implicam uma ingerência na informação corporal ou no corpo humano, e noutra dimensão, podemos referir aqueles métodos que implicam um grau de interação ou provocação, com o investigado.

Identificamos assim, em primeiro lugar, os métodos ocultos de investigação de dados de identificação e de localização de pessoas e bens. Este tipo de investigação é possível, devido ao fato dos equipamentos ou terminais de informação e comunicação possuírem, eles próprios, um esquema de identificação e localização, que pode ser conseguido por meio do acesso às redes de comunicações eletrónico-digitais a que estes se encontram interconectados ou, ainda, em alguns casos, fora do contexto eletrónico-digital, em si mesmos, dados os elementos que o terminal detém e que, por via de certas técnicas de investigação, podem ser captados e obtidos à distância.[71]

Podemos então elencar, como métodos ocultos de investigação de dados de identificação e localização de pessoas e bens, a investigação oculta por localização e identificação de dados celulares, os quais ainda se subdividem, a título de exemplo, na obtenção e junção de dados de localização[72], a obtenção de dados de localização celular no âmbito da atividade de prevenção criminal ou das medidas cautelares de polícia[73] e a obtenção e junção dos registos da realização de conversações ou comunicações[74]. Ainda fazendo parte do elenco deste tipo de meios, encontramos a investigação oculta por localização e identificação de dados a partir do sistema de GPS, GMS, IMSI *catcher* ou VBTS, estes, também, se dividem na investigação oculta por localização e identificação de dados por meio de equipamento de GPS amovível, a localização e identificação de dados por meio de equipamento com tecnologia de GPS não amovível ou fixo, em chapa de matrícula ("chip" de matrícula), a localização e identificação por meio de IMEI ou IMSI

[71] Benjamim Silva Rodrigues, "Da Prova Penal – Tomo II...", páginas 84 e 85.
[72] Ex vi artigo 189.°, n.°2, 1.ª parte, do CPP, em qualquer fase do processo, mediante ordem ou autorização judicial.
[73] Artigo 252.°-A, do CPP.
[74] Ex vi artigo 189.°, n.°2, 1.ª parte, do CPP, em qualquer fase do processo, mediante ordem ou autorização judicial.

do equipamento de informação e comunicação ou de endereço de IP, e por último, a localização e identificação por meio de vigilância informática de movimentos de fluxos económico-financeiros em contas bancárias, tendo sempre em conta o condicionalismo legal da quebra do sigilo bancário.

Em segundo lugar, encontramos os métodos ocultos e investigação criminal com infiltração ou provocação junto do visado, suspeito ou arguido, dos quais o principal exemplo são as ações encobertas, consagradas na Lei n.º 101/2001 e a utilização de agente ou funcionário infiltrado, prevista nos artigos 59.º e 59.º-A, do Decreto-Lei n.º15/1993, Legislação de Combate à Droga[75].

Em terceiro lugar, podemos referir os métodos ocultos de investigação criminal com ingerência corporal ou em "informação corporalmente obtida", sendo claro exemplos destes, as perícias de ADN enquanto técnica de identificação e investigação criminal, através da fixação e comparação de perfis de ADN. Previstas na Lei n.º5/2008, de 12 de fevereiro, (e na Lei sobre a informação genética pessoal e informação de saúde – Lei n.º12, de 26 de janeiro) e, ainda, na Deliberação n.º 31191/2008, do Instituto Nacional de Medicina Legal, I.P., que aprova o Regulamento do Funcionamento da Base de Dados de Perfis de ADN e também o controlo de álcool ou substâncias psicotrópicas sem o consentimento, estado de inconsciência ou excesso de consentimento presumido, ou contra a vontade do visado.

4.2.1. Ações encobertas

Cabe-nos neste subcapítulo falar e explicar a utilização de ações encobertas previstas no artigo 19º da Lei do Cibercrime, e, consequentemente, na Lei n.º 101/2001, por remissão do primeiro artigo. Esta utilização surge com o objetivo de combater as dificuldades nos meios de obtenção de prova em crimes, como o tráfico de estupefacientes e ainda em crimes informáticos. A dificuldade em obter as provas necessárias para a descoberta da verdade material, torna necessária a integração de pessoas, os chamados agentes infiltrados, para que as investigações possam assim desenrolar-se da forma mais diligente possível.

O surgimento deste instituto, não está livre de discussão, principalmente no que diz respeito aos métodos proibidos de prova, visto que é exatamente esta proibição que vai balizar toda a atuação que o agente infiltrado terá. Assim, as ações encobertas devem assentar, em determinadas exigências e pressupostos materiais, formais-procedimentais e orgânicos, devido a

[75] Alterado sucessivamente, sendo a ultima alteração a Lei n.º 7/2017, de 02/03.

variados aspetos, sendo um deles o facto de serem suscetíveis a violar uma enorme panóplia de interesses e direito legalmente consagrados.

As ações encobertas vêm-se então balizadas por duas finalidades do DPP. Por um lado, a descoberta da verdade material, intrínseca à obtenção dos meios de prova, que preza por uma maior eficácia e segurança na aplicação da justiça. Por outro lado, a defesa e proteção dos direitos e interesses legalmente consagrados, que são postos em causa por este meio de obtenção de prova, sendo claro exemplo disso, o direito ao silêncio e o direito ao não testemunho. Tal, como todos os outros meios de obtenção de prova ocultos, é necessário dar uso ao princípio da proporcionalidade, onde se pondera entre a necessidade, a adequabilidade e a proporcionalidade *stricto sensu*. Posto isto, concluímos que apenas na criminalidade mais grave ou mais complexa, se pode dar uso a este método oculto de obtenção de prova.

Segundo Costa Andrade o uso de ações encobertas com finalidade meramente repressiva não se mostra admissível, traduzindo-se esta atuação num meio enganoso e, como tal, a prova obtida através da sua atuação é nula. Só admitindo a ação encoberta para fins exclusivos ou essencialmente preventivos, quando se estiver perante a criminalidade mais grave.[76] Rui Pereira[77], também, destaca esta vertente preventiva, de modo a evitar-se a ocorrência de futuros crimes, sendo a utilização deste agente admitida desde que a causa justificativa de utilização, possa basear-se em, evitar a ocorrência de um crime e esteja, sempre, conforme o princípio da proporcionalidade.

4.2.2 Agentes encoberto (infiltrado vs provocador)

A figura do agente infiltrado está hoje em dia consagrada em praticamente todos os ordenamentos jurídicos, principalmente nos europeus. Contudo esta figura e o uso de outros meios preventivos do crime, como por exemplo, a observação contínua de um indivíduo ou a vigilância eletrónica, tem suscitado bastante discussão doutrinária. Mas o nono congresso das Nações Unidas para a prevenção do crime e tratamento dos delinquentes, que teve lugar na cidade do Cairo de 29 de abril a 8 de maio de 1995, declarou que a polícia e outros serviços de ordem pública, têm de se socorrer das novas tecnologias de ponta, como meio necessário para o combate eficaz da criminalidade organizada.[78]

[76] Costa Andrade, "Sobre as proibições de prova em processo penal", (Coimbra: Coimbra Editora, 2013).

[77] Rui Pereira, "O "agente encoberto" na ordem jurídica portuguesa", in Medidas de Combate à Criminalidade Organizada e Económico-Financeira, Centro de Estudos Judiciários, (Coimbra: Coimbra Editora, 2004), páginas. 11 e ss..

[78] Isabel Oneto, "O Agente Infiltrado – Contributo para a compreensão do regime jurídico das ações encobertas", (Coimbra: Coimbra Editora, 2005), páginas 264.

Agente infiltrado é aquele agente de autoridade, funcionário de investigação criminal ou um cidadão particular, como terceiro, mas que atua sempre de forma concertada com a Polícia Judiciária, que, sem revelar a qualidade e identidade em que atua, mantem-se a par dos acontecimentos, acompanha a execução dos factos, pratica atos de execução se for necessário, de forma a obter provas para a incriminação do suspeito ou dos suspeitos.[79] Assim, o agente infiltrado vai ganhando a confiança dos suspeitos, para melhor os observar e obter informações relativas às atividades criminosas dos suspeitos ou do suspeito e obter provas contra estes, tendo sempre em conta as finalidades exclusivas de prevenção ou repressão criminal, sem contudo determinar os suspeitos à prática de novos crimes. Portanto, agente infiltrado é alguém que recorre a estratégias para manipular indivíduos. Podemos afirmar que as ações encobertas, não são mais que um envio de alguém para o mundo do crime, sendo que este vai desenvolver relações pessoais e sociais, que podem conduzir a uma certa distorção do raciocínio e assim envolver o agente numa nova realidade e numa nova dimensão. Há uma linha muito ténue entre a desresponsabilização criminal dos agentes, em certas condutas, e a já responsabilização criminal de condutas mais graves e ilícitas.

O principal objetivo do agente infiltrado é a obtenção de prova e consequentemente a descoberta da verdade material, para tal, deve mantêm-se a par dos acontecimentos e até prevenir certas situações ilícitas de acontecer, ou seja, manter-se à parte e não provoca para conseguir criar prova, não incentiva alguém a praticar atos ilícitos, que, deste modo ou noutras, circunstâncias, não teria praticado.

A coautoria e a cumplicidade são as únicas atividades de infiltração que são permitidas ao agente infiltrado[80]. Apenas é permitido, e no caso da atividade criminosa já estar em curso, colaborar na atividade criminosa desenvolvida pelos respetivos agente, presentando-lhes designadamente auxílio material ou moral[81], ou até mesmo praticar atos de execução do crime. Voltamos a referir que é necessário que a atividade criminosa já esteja em curso, e o agente infiltrado nunca pode adotar uma conduta de impulso ou instigação dessa atividade, sob a pena de transpor a linha ténue e se transformar num agente provocador. Portanto não pode o agente determinar a prática do crime. Um caso bastante conhecido em Portugal é o caso Teixeira de

[79] A dissimulação da identidade e/ou qualidade do agente pode fazer-se das mais diversas formas, sendo exemplos destas, a apresentação como um vulgar delinquente, ou mesmo apresentar uma nova identidade e ainda ocultar a verdadeira identidade, fazendo-se passar por um cidadão particular e não um agente policial.

[80] Rui Pereira, "O Agente Encoberto...", páginas 30 e 32-33.

[81] Artigo 26.º, número 1, do CP.

Castro[82], no qual (de forma resumida), o Estado Português foi condenado a pagar uma indemnização pelo Tribunal Europeu dos Direitos do Homem, a um cidadão português.

Rui Pereira considera que a atuação do agente infiltrado não viola a integridade moral da pessoa[83], e concordamos com esta opinião, uma vez que olhando para a atuação deste agente, não vemos como poderão estas ações conflituar com o direito à integridade moral. Quando essas ações conflituarem com esse direito já não estaremos perante o agente infiltrado mas face ao agente provocador.

Mais uma vez, utilizamos a descoberta da verdade material, como justificação para um meio oculto de investigação criminal, ou seja, para o uso do agente infiltrado. Julgamos deveras importante, referir a figura do agente provocador, visto que a utilização dos agentes infiltrados pode levar a que a pessoa em causa abuse da limitação[84] decorrente deste método, surgindo então a figura de agente provocador, levando a condutas indesejadas, exageradas e onde é ultrapassada a linha ténue da conduta do agente encoberto/infiltrado. O agente provocador é pois aquele que tem uma intervenção instigadora de forma a criar prova, estimulando outrem a praticar certo ilícito criminoso, que sem esse incentivo certamente não o iria realizar. Logo, o agente provocador cria o próprio crime e o próprio criminoso, porque induz o suspeito à prática de atos ilícitos instigando-o e alimentando o crime, agindo, nomeadamente, como comprador ou fornecedor de bens ou serviços ilícitos.

Em suma, o agente provocador é aquele que, sendo uma entidade policial ou um cidadão particular, mas sempre ligado à Polícia Judiciária, convence outrem à prática do crime, não querendo o crime em si, mas sim pretendendo submeter esse suspeito a um processo penal, que consequentemente, e em último caso, vai levar a uma pena. Estamos perante a possibilidade do agente provocador, que atua com dolo, induzir outrem à prática do crime, não na perspetiva da realização do crime como fim em si, mas sim a realização deste como fim de submeter o provocado a um processo penal. A atuação do agente provocador não é o mais relevante, podemos pois, estar perante qualquer ação idónea de convencimento do provocado à prática do crime, seja essa um incitamento expresso, um pedido ou qualquer outra forma de comunicação.

---

[82] Joana Tocantins Santos, "Investigações Criminais Encobertas- Da evolução do Regime Jurídico das Ações Encobertas ao equilíbrio das finalidades do Processo Penal no uso do Agente Encoberto", (Dissertação de Mestrado, 2016), página 10.

[84] A utilização deste tipo de agente limita em grande parte direitos, liberdades e garantias por ser um meio oculto de obtenção de prova.

4.2.2.1 Punibilidade do agente encoberto (infiltrado vs provocador) e valoração das provas por este obtidas

Importa agora nos centrarmos em duas questões, sendo a primeira uma questão substantiva, ou seja, saber ou não se o agente provocador praticou uma ação típica, ilícita, culposa e punível, e se deve ser punido ou não. Já a segunda questão é a de saber, se deve-se valorar ou não os elementos de prova obtidos pelo agente provocador. No que diz respeito a esta ultima questão, trataremos dela mais adiante. Contudo cabe-nos agora falar da primeira questão.

Existem variadas teorias sobre se o agente provocador deve ser punido ou não. Em primeira análise, podemos verificar que visto que o agente provocador não deseja o crime em si, mas apenas a condenação do provocado, não deve a conduta do agente relevar, visto que segundo o artigo 13.º do CP, não pode ser responsabilizado penalmente aquele que age sem dolo. Já no que diz respeito, à punibilidade do agente provocador como agente instigador, este deve em regra ser punido, devido às regras da punibilidade da instigação ditadas pela acessoriedade limitada[85]. Contudo, o que se censura no direito penal é a violação de um bem jurídico protegido, sendo que a questão da punibilidade do agente provocador deve ser vista como uma posição, particular, do agente, perante um bem jurídico-penal, posição essa que não é de desrespeito, nem de indiferença, porque o agente de autoridade pública, (ou até mesmo o terceiro, ancorado pela Polícia Judiciária) atua de maneira, mesmo, não sendo esta a mais correta, a combater o crime, reafirmando os valores da sociedade e os bens jurídicos do ordenamento.

Cabe-nos fazer menção ao agente encoberto. Este é um agente da autoridade, ou um cidadão particular que atua de forma concertada com a Polícia Judiciária, que sem revelar a sua identidade ou qualidade, frequenta meios conotados com o crime na esperança de descobrir possíveis criminosos. Ao contrário do agente provocador, este não instiga ao crime, e diverso do agente infiltrado, não tem como principal função ganhar a confiança de ninguém. Então, a sua presença e a sua qualidade não vão determinar o rumo dos acontecimentos, sendo indiferente este estar presente ou não para certo ilícito acontecer. Podemos afirmar que se trata do vulgarmente conhecido "polícia à paisana". A atuação destes é totalmente lícita e legalmente admitida ao abrigo do princípio da oficialidade, da investigação, da liberdade e atipicidade dos meios de prova não proibidos. Por exemplo, se este for intercetado por um traficante, que lhe proponha a aquisição de estupefacientes, estamos perante um agente encoberto, se pelo contrário

[85] Segundo esta teoria, a participação é penalmente relevante quando o agente contribui para a prática de um facto típico e ilícito. A diferença entre a acessoriedade mínima e a limitada é que, na primeira, basta o facto ser típico para existir participação, já na segunda, a participação depende da tipicidade e ilicitude do facto.

for o agente a instigar o traficante a vender-lhe estupefacientes, já estamos perante um agente provocador.

A figura de agente infiltrado não tem previsão no CPP, e na CRP, podemos afirmar que apesar de não se encontrar expressamente consagrada, pode admitir-se a sua previsão, como meio necessário, a fim de prevenir e reprimir as formas de criminalidade mais graves e que violam direitos fundamentais, como o direito à vida, o direito à integridade física e o direito à liberdade e segurança. Contudo, é necessário, para a admissibilidade processual desta figura como meio de obtenção de prova, que esta esteja expressamente consagrada na lei. Atualmente a lei que regula as ações encobertas é a Lei nº101/2001, mas antes da publicação e entrada em vigor desta, houve algumas leis precedentes, que já defendiam a ideia de ações encobertas e do agente infiltrado. A Lei do combate ao tráfico e consumo de estupefacientes e substâncias psicotrópicas,[86] no número 1 do seu artigo 59.º e a Lei de combate à corrupção e criminalidade económica e financeira, no seu artigo 6.º,[87] foram as primeiras a consagrar a figura de agente infiltrado.

A Lei nº45/96, de 3 de setembro, veio após as acima referidas, alargar mais uma vez o âmbito de atuação do agente infiltrado na prevenção e repressão dos crimes de tráfico de estupefacientes e substancias psicotrópicas. Nessa mesma lei, na epígrafe do artigo 59.º -A, faz-se pela primeira vez, no ordenamento jurídico português, menção à figura de agente infiltrado. Mais uma vez, esta lei faz referência à não punibilidade do agente, no número 1 do artigo 59.º.[88] Além de que, no número 2 do mesmo artigo, afirma-se a obrigatoriedade da prévia autorização da entidade judiciária competente, para o uso deste método de obtenção de provas e, para garantir a sua validade.

Apenas nestes casos, é permitida a figura de agente infiltrado, sendo as provas obtidas de outra forma, consideradas proibidas, de acordo com o prescrito no artigo 125.º do CPP, onde se afirma que só são admissíveis provas que não forem proibidas pela lei do combate à corrupção e criminalidade económica e financeira, sendo que a figura do agente infiltrado, exceto no previsto nos artigos acima referidos, é legalmente inadmissível, por isso mesmo ilícito. Além, de que, perante a alínea a) do número 2 do artigo 126.º, também ele do CPP, as provas obtidas por meios enganosos, são nulas, e sem qualquer utilidade.

[86] Decreto-Lei n.º 15/93, de 22 de janeiro.

[87] Lei n.º 36/94, de 29 de setembro, alterado pela Leo nº. 90/99, de 10 de julho.

[88] " Não é punível a conduta de funcionário de investigação criminal ou de terceiro atuando sob controlo da Polícia Judiciária que, para fins de prevenção ou repressão criminal, com ocultação da sua qualidade e identidade, aceitar, detiver, guardar, transportar ou, em sequência e a solicitação de quem se dedique a essas atividades, entregar estupefacientes, substâncias psicotrópicas, precursores e outros produtos químicos suscetíveis de desvio para o fabrico ilícito de droga ou precursor.".

O primeiro artigo da Lei do combate à corrupção e criminalidade económica e financeira que referimos supra, no seu número 1, consagra a noção de agente infiltrado em cima enumerada, contudo, é de salientar, que a atuação do funcionário de investigação criminal que, por iniciativa própria, vende e consequentemente entrega droga para identificar consumidores, fornecedores ou compradores, com o objetivo de os perseguir criminalmente, é ilícita e por isso possivelmente punível. Estamos, pois, perante um caso de agente provocador e não agente infiltrado.

Esta proibição de valoração da prova é quase absoluta, visto encontrarmos uma exceção no número 4 do artigo 126.º do CPP. Esta não valoração das provas obtidas por um agente provocador leva a que estas sejam desanexadas do processo, visto que apenas serviriam para que o juiz tivesse conhecimento de uma situação que não poderia conhecer. Existe, porém, o chamado efeito-à-distancia que advêm da questão da nulidade e não valoração das provas obtida através de ações do agente provocador. Assim, é necessário saber se a proibição deve circunscrever-se à valoração do meio de prova diretamente obtido a partir da violação da lei ou, pelo contrário, se há-de comunicar a todos os demais meios de prova que teriam sido obtidos sem meio de prova ilegalmente obtido, dito por outras palavras, se as provas se sustentam em meios de obtenção proibidos, devem ser nulas.

Importa aqui, fazermos um pequeno à parte, de forma a explicarmos o consagrado no artigo 126.º do CPP. No n.º 1 deste artigo estabelece-se a nulidade das provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas. Já, o n.º 2 do referido preceito enumera as situações nas quais se considera existir uma ofensa à integridade física ou moral das pessoas.[89] É precisamente na categoria de meios enganosos que se encontra o fundamento da nulidade das provas obtidas pelo agente provocador.

As proibições constantes no artigo 126.º do Código de Processo Penal podem ser definidas como absolutas ou relativas. Na primeira categoria cabem as referidas nos números 1 e 2 do artigo 126.º, pois as provas assim obtidas, por atentarem contra direitos tidos como intrespassáveis para o próprio titular (o seu consentimento, é, portanto, irrelevante), consideram-se proibidas em termos absolutos, não podendo, em caso algum, ser utilizadas no processo. Já as proibições relativas dizem respeito aos casos em que se utilizam processos de recolha de provas com intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, sem o consentimento dos seus titulares, conforme dispõe o n.º 3 do mesmo

[89] São essas a "perturbação da liberdade de vontade ou de decisão através de maus tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos".

artigo. Nesta caso, não existe uma proibição de carácter absoluto, uma vez que o legislador considera que os direitos em causa são disponíveis e que a prova é válida mediante consentimento do seu titular.

Apesar disso, quer o número 1 e 2, quer o número 3 do artigo 126.º do CPP tem a mesma sanção, não determinando a diferente densidade das proibições para a nulidade decorrente da sua violação, ou seja, apesar de no número 1 estarmos perante direitos irrestritíveis e no número 3 estarmos perante direitos restritíveis, este critério não leva a que se deva aplicar duas modalidades de nulidade distintas.

Assim, as nulidades das provas obtidas com recurso aos métodos ilícitos elencados quer no n.º 1, quer no n.º 3 do artigo 126.º, são nulidades com um regime análogo ao das nulidades insanáveis, sendo que e se por um lado, também elas são de conhecimento oficioso e insuscetíveis de sanação, por outro lado têm algumas diferenças do regime geral das nulidades insanáveis que permitem tratá-las como uma modalidade *sui generis* desta. As principais diferenças passam pelo tempo da sua arguição e pela possibilidade de utilização das provas. Sendo que, como tal, não podem ser utilizadas no processo, com exceção do caso referido no n.º 4[90].

Respondemos nestes parágrafos antecedentes, à segunda questão que abordámos anteriormente, ou seja, se deve-se valorar ou não os elementos de prova obtidos pelo agente provocador. Concluímos que estando perante provas obtidas por instigação e por meios ocultos de obtenção de prova, que estas se encontram na categoria das provas proibidas e por essa mesma razão são nulas. Cabe-nos agora, considerando esta temática relevante para a dissertação que apresentamos, saber se as provas obtidas por um agente infiltrado podem ser valoradas ou não.

Em primeiro lugar, já sabemos que a atuação do agente infiltrado pressupõe uma restrição a direitos e interesses fundamentais da pessoa humana e que os agentes do crime estão a ser induzidos e traídos pelo infiltrado, assim sendo podemos considerar que o agente infiltrado deva integrar a categoria dos meios de prova relativamente proibidos.[91] Estamos perante uma verdade incontestável, que a atividade de um agente infiltrado implica um processo de secundarização de certos direitos e interesses constitucionalmente consagrados, sendo por isso um meio oculto de obtenção de prova. Mas é de salientar, que este método, nunca pode pôr em causa direitos ou garantias fundamentais diretamente ligados com a personalidade humana. Por tal, é deveras

[90] As provas obtidas por um método proibido "podem (...) ser utilizadas com o fim exclusivo de proceder contra os agentes do mesmo.".
[91] Artigo 32.º, n.º8, da CRP em conjugação com o artigo 126.º, n.º2, do CPP.

complicado achar um equilíbrio entre o uso destes métodos ocultos de obtenção de prova e a violação de direitos fundamentais, pois tem-se como fim a descoberta da verdade material, para que se possa fazer justiça, sempre equilibrado com o princípio da proporcionalidade nas suas três dimensões.

Em segundo lugar, temos de verificar quando é que a intromissão na vida privada, ou seja, a intrusão decorrente dos atos do agente infiltrado, pode ser considerada abusiva, e por isso, as provas que nesta são obtidas, serão consideradas nulas.

Podemos elencar quatro momentos:

- O primeiro é quando a intromissão é feita fora dos casos previstos na lei e sem intervenção judicial;

- O segundo momento é quando esta é desnecessária;

- Esta forma de ser desproporcionada é também uma das razões para ser considerada abusiva;

- Sendo que quando aniquila os próprios direitos é o ultimo momento que vamos enumerar.

A primeira razão que elencamos, é a não previsão na lei, e, apesar disso, obter-se na mesma a prova, quando a previsão/autorização é um pressuposto legal obrigatório. É, portanto, necessário, quer seja direta ou indiretamente a autorização constitucional para o uso deste método oculto de obtenção de prova.

Portanto, sempre que a Constituição não preveja, aliás, sempre que a intromissão decorrente da atividade do agente infiltrado não se faça nos casos e nos termos em que a Lei Fundamental admite a restrição dos direitos, estamos perante uma intromissão abusiva. O agente infiltrado é uma figura que hoje em dia tem assento legal, contudo e apenas, na conformidade com essas leis, as provas obtidas por estes poderão ser válidas e sujeitas a valoração. Todas as outras serão consideradas provas proibidas e por consequência nulas.

Não é por certo meio de obtenção de prova estar previsto na lei, que se pode usá-lo indiscriminadamente. Assim sendo, é necessário para o recurso ao uso deste método oculto de obtenção de prova, que seja cumprido o requisito constitucional da necessidade, previsto no número 2 do artigo 18.º da CRP. As restrições aos direitos fundamentais, devem ser limitadas, sempre ao necessário, para salvaguardar outros direitos ou interesses constitucionalmente protegidos, afirma este artigo. Neste caso, em concreto, só se poderão pôr em causa direitos fundamentais quando tal for exigido pelo dever de administração da justiça, previsto no artigo

202.º da CRP. Então, esta intromissão só poderá ser considerada, não abusiva, se esta for o único meio de administrar a justiça e de resolver o caso em concreto. Mesmo dentro do CPP, na alínea c) do número 1 do artigo 179.º, e no número 1 do artigo 187.º, no que diz respeito à apreensão de correspondência e às escutas telefónicas, estes preceitos afirmam, que estes meios de obtenção de prova só podem ser autorizados, se houver "razões para crer que a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova". Mais uma vez aqui, estamos perante o princípio da necessidade.

O princípio da proporcionalidade, já conseguimos concluir isso, é uma das pedras basilares de quase todos os ramos de direito e todas as esferas jurídicas. Assim, não basta a prova ser necessária, para se abrir mão dos direitos constitucionais e portanto obter-se a prova por qualquer meio. É, imprescindível pesar na balança o bem jurídico que se irá sacrificar e o interesse que, em concreto, se pretende alcançar. Temos de analisar, sempre cada caso em concreto, a gravidade do crime e as suas consequências, para assim se habilitar ou não o uso destas formas de obtenção da prova.

Como último momento apresentamos a proteção do núcleo essencial do direito, ou seja, existem direitos, liberdades e garantias que não podem ser violados, e, por isso, a restrição prevista no número 3 do artigo 18.º da CRP, não se pode aplicar a estes. A necessidade e a proporcionalidade serão, elas próprias, a ditar os contornos deste núcleo essencial. Contudo, temos de ter em atenção que, estas, nunca poderão levar a um sacrifício total deste núcleo.

Nos dias de hoje, a lei que regula as ações encobertas é a Lei nº101/2001, vindo alargar o âmbito destas e impor-lhes limites e revogando os artigos 59.º e 59.º-A da Lei n.º 15/93, de 22 de janeiro, e o artigo 6.º da Lei n.º 36/94, de 29 de setembro. Assim sendo, o primeiro artigo surge como um limite à utilização deste instituto, sendo uma proteção para os excessos possíveis, ainda clarificando a distinção entre agente infiltrado e agente provocador. Ainda neste artigo, se alarga a intervenção das ações encobertas, através da admissão da utilização destas, numa fase de pré-inquérito, incluindo a prevenção no seu objeto, ao contrário da sua limitação à investigação criminal. No número 2 deste artigo, que encontramos uma noção para o conceito de ação encoberta.[92]

[92] "Consideram-se ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade."

O artigo 2.º da presente lei alarga claramente o catálogo de crimes, que podem ser sujeitos ao uso de ações encobertas. No elenco de crimes, que podem ser sujeitos ao uso de ações encobertas, encontramos:

- O homicídio voluntário, desde que o agente não seja conhecido;

- Os crimes contra a liberdade e contra a autodeterminação sexual a que corresponda, em abstrato, pena superior a 5 anos de prisão, desde que o agente não seja conhecido, ou sempre que sejam expressamente referidos ofendidos menores de 16 anos ou outros incapazes;

- Os crimes relativos ao tráfico e viciação de veículos furtados ou roubados; a escravidão, o sequestro e o rapto ou a tomada de reféns;

- O crime de tráfico de pessoas; as organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo;

- A captura ou atentado à segurança de transporte por ar, água, caminho-de-ferro ou rodovia a que corresponda, em abstrato, pena igual ou superior a 8 anos de prisão;

- Os crimes executados com bombas, granadas, matérias ou engenhos explosivos, armas de fogo e objetos armadilhados, armas nucleares, químicas ou radioativas;

- O roubo em instituições de crédito, repartições da Fazenda Pública e correios; as associações criminosas;

-Os crimes relativos ao tráfico de estupefacientes e de substâncias psicotrópicas; o crime de branqueamento de capitais, outros bens ou produtos;

- A corrupção, o peculato e a participação económica em negócio e tráfico de influências;

- A fraude na obtenção ou o desvio de subsídio ou subvenção;

- Todas as infrações económico-financeiras cometidas de forma organizada ou com recurso à tecnologia informática; todas as infrações económico-financeiras de dimensão internacional ou transnacional;

- A contrafação de moeda, títulos de créditos, valores selados, selos e outros valores equiparados ou a respetiva passagem;

- Os crimes relativos ao mercado de valores mobiliários.

Este leque de crimes é bastante ambíguo e heterogéneo, principalmente no que diz respeito ao bem jurídico que tutelam, que vai desde o homicídio, ao tráfico e ainda a variados crimes fiscais. Esta variedade podemos justificá-la com a realidade do quotidiano, onde nos deparamos com uma criminalidade mais complexa e oculta, que precisa de ser acompanhada por métodos de investigação também eles mais complexos e por vezes, ocultos.

A lei, tal como em todos os casos em que há a possibilidade de violação de direitos e interesses consagrados legalmente, prevê a instrumentação basilar do princípio da proporcionalidade para, se averiguar o uso ou não das ações encobertas, como meio de obtenção de prova. Sendo sempre necessária a autorização, supervisão e controlo jurisdicional tanto à *priori* como à *posteriori*, deste método de investigação criminal.

Os requisitos necessários à atualização deste método oculto de obtenção de prova, estão previstos no artigo 3.º deste mesmo diploma. São basicamente os mesmos, que já foram enumerados no início deste capítulo, no que diz respeito aos meios ocultos de obtenção de prova em geral. Contudo, nunca é demais afirmarmos que a adequação aos fins de prevenção e repressão criminal deve ser sempre analisada ao caso em concreto e sempre ancorada pelo princípio da proporcionalidade. O número 3, do mesmo artigo, defende que ninguém deve ser obrigado a participar na ação encoberta, não se violando assim nenhum direito fundamental, como a liberdade.

A prévia autorização judicial é sempre necessária. Sendo dada por uma magistrado do MP, e depois comunicada ao juiz de instrução, excetuando os casos em que as ações encobertas decorram no âmbito da prevenção criminal. Nessa situação a autorização advém de um JIC, mediante proposta do MP. Estes procedimentos estão consagrados nos números 3, 4 e 5 do artigo 3.º da Lei das Ações Encobertas.

Mais uma das inovações que o regime que este diploma transporta, que podemos referir, é a plasmada no artigo 5.º, ou seja, a figura da identidade fictícia. Esta é restringida aos agentes da polícia criminal que participem nas ações encobertas. Esta identidade fictícia é atribuída por despacho do Ministro da Justiça, mediante proposta do diretor nacional da PJ. A validade desta é de seis meses, que podem ser prorrogáveis por períodos de igual duração, admitindo-se o seu uso, não apenas, no exercício concreto da investigação, mas, também, em todas as circunstâncias do tráfico jurídico e social.

Já no que diz respeito, à isenção da responsabilidade do agente, esta encontra-se consagrada no artigo 6.º do diploma em análise. Aqui determina-se que, não pode "ser punível a conduta do agente encoberto que, no âmbito de uma ação encoberta, consubstancie a prática de atos preparatórios ou de execução de uma infração em qualquer forma de comparticipação diversa, da instigação e da autoria mediata, sempre que guarde a devida proporcionalidade com a finalidade da mesma".

4.3. Utilização de *malware* como meio de obtenção de prova digital

Antes de nos debruçarmos, sobre a resposta concreta, à possibilidade ou não de utilização de *malware* como meio de obtenção de prova digital, cabe-nos, falar, do Direito Processual Penal. Este merece, por parte do legislador constitucional, uma particular atenção, porque o seu objeto, e o conjunto de medidas e expedientes, que alguns sujeitos processuais podem lançar mão, podem acarretar uma violação ou séria colocação em perigo, de direitos e interesses fundamentais da pessoa humana.

Podemos afirmar que ancorados um pouco por esta preocupação, encontramos um ramo do direito, o Direito Constitucional Penal.

O DCP está interligado a um conteúdo específico do poder estatal, enquanto *jus punendi*, e não apenas inerente à realização da justiça intersubjetiva e dos fins ou interesses da Sociedade. Há, pois, a necessidade de uma justificação desse poder estatal, sendo que o julgamento de constitucionalidade como juízo sobre a compatibilidade com princípio e normas constitucionais de normas ou decisões penais e o juízo correspondente à não observância, de natureza omissiva dos princípios e normas constitucionais, vinculantes em certa matéria, são hoje em dia aspetos a ter em conta, quando se trata desta temática.

O legislador encontra-se, a nosso ver, sob o ponto de vista constitucional, duplamente vinculado. Em primeiro lugar, quando se dirige à comunidade jurídica em geral, e através de princípios fundamentais como a dignidade da pessoa humana ou da igualdade, deparando-se com uma vinculação a estes.

Já em segundo lugar, o legislador depara-se com uma vinculação a princípios que só aos sujeitos processuais, como o MP ou o JIC dizem respeito, ou seja, o legislador constitucional, dirige-se ao legislador processual penal, em concreto, e aos sujeitos que importam para a investigação criminal.

A obtenção de provas envolve constrangimento, restrição ou limitação dos direitos fundamentais. Entende-se, por isso, a mesma obtenção deve ser levada a cabo em determinado condicionalismo garantístico. Assim, é necessário, no momento em que houver restrição de direitos fundamentais, que, coexista uma lei que expressamente autorize tal. A ausência desta lei, e temos de ter em atenção que esta deve fornecer um regime detalhado acerca dos meios de investigação limitadores de direitos, pode significar uma privação ao juiz, de critérios de

racionalidade necessários, para resolver o conflito entre direitos do possível arguido violados e o interesse publico da descoberta da verdade.

Assim as leis que vão autorizar a restrição, constrangimento ou limitação de direitos fundamentais, necessariamente tem de cumprir quatro requisitos[93]: Em primeiro lugar a lei tem de ser prévia ao momento em que se dá a restrição do direito fundamental. Tem de ser escrita, afastando qualquer limitação oral que possa existir. E por fim, deve ser certa e estrita, ou seja, a lei não pode ser vaga e deve-se cingir ao estritamente essencial, para salvaguardar o núcleo e outros direitos fundamentais envolvidos em tal limitação ou restrição.

Deparamo-nos, mais uma vez, com o respeito pelo princípio da legalidade, visto que, este em matéria constitucional-penal dota os cidadãos de uma segurança jurídica que lhes permite tomar consciência e conhecimentos das condutas relevantes jurídico-penalmente e das suas respetivas consequências jurídicas.

Aos tribunais, e consequentemente no que diz respeito ao tema que estamos a tratar, aos JIC´s é colocado sobre os ombros pela CRP, o dever de assegurar a defesa dos direitos e interesses legalmente protegidos dos cidadãos, nomeadamente, mediante a repressão da violação da legalidade democrática e resolução dos conflitos, entre interesses públicos e privados, como podemos verificar no número 2 do artigo 202.º da CRP.

Ainda na CRP, o número 4 do artigo 32.º (*a contrario sensu*) refere que a instrução criminal pertence a um juiz e que a delegação de tarefas noutras entidades, por este são proibidas, caso tais atos poderem diretamente contender com os direitos fundamentais. Assim, e seguindo a linha constitucional, podemos encontrar no CPP, os atos que o JIC deve praticar[94] e os atos que este mesmo deve ordenar ou autorizar[95].

O número 1 do artigo 205.º da CRP exige que "as decisões dos tribunais que não sejam de mero expediente são fundamentadas na forma prevista na lei". Verificamos, pois, que no caso de autorização do juiz da utilização de um meio oculto de obtenção de prova, deve ser fundamentado expressamente e acessível ao homem médio, que passou a configurar como um verdadeiro direito fundamental da pessoa, cujos direitos são alvo da medida de limitação ou restrição no âmbito de um processo criminal. Estamos, portanto, perante uma garantia constitucional de grande importância para o sujeito dos direitos lesados.

[93] "*Lex previa, scripta, certa e stricta*".
[94] Artigo 268.º do CPP.
[95] Artigo 269.º do CPP.

No nosso ordenamento jurídico, mais precisamente na CRP, consagra-se no seu artigo 18.º a regra da proporcionalidade em sentido amplo, que se vai dividir em três ideias fundamentais, as quais já tratámos nesta dissertação. São elas a adequação, a necessidade e a proporcionalidade em sentido restrito. Esta proporcionalidade vai configurar-se como a "trave mestra" de legitimação do *ius punendi* estatal e, consequente, como, restrição dos direitos fundamentais. Será a existência de proporcionalidade que advém das diretrizes constitucionais que dar resposta à questão que discutimos nesta exposição. Se é ou não possível a utilização de *malware* como método oculto de obtenção de prova.

O princípio da proporcionalidade leva, então, a que se alcance um justo equilíbrio entre os vários direitos e interesses legalmente protegidos. É necessária a exigência de uma mediação, no momento em que o legislador cria as normas jurídicas, que vão entrar em discórdia com outras já existentes no ordenamento, dos interesses que estão em conflito, de maneira a pesar cada um deles e encontrar uma solução que permita garantir a subsistência, dos valores fundamentais à vida num estado social de direito.

A primeira ideia fundamental que advêm do princípio da proporcionalidade é o princípio da adequação ou idoneidade da medida. Aqui, é necessário, que haja uma relação de adequação entre o meio usado e o fim perseguido. Não é suficiente, apelar para um determinado bem jurídico protegido, para legitimar uma violação de um direito, por exemplo, como numa intervenção corporal na recolha de ADN. Urge que a restrição, levada a cabo, seja apropriada e útil para lograr o fim que justifica a limitação do direito. Posto isto, a razão pela qual, se vai violar o direito, tem de ser apropriada, idónea e adequada para atingir o fim (normalmente um interesse publico superior) que se pretende obter, mediante tal restrição ou limitação ao direito fundamental. Esta ideia pode fundamentar-se no número 1 do artigo 193.º do CPP[96] e também no princípio da proibição do excesso, plasmado no número 2 do artigo 18.º da CRP[97].

A segunda ideia fundamental que expomos é o princípio da necessidade ou indispensabilidade da medida. Nesta ideia, já apresentada anteriormente, afirma-se que existindo outras medidas investigatórias, ou outros métodos para obter a prova, que possam garantir de forma satisfatória, o objetivo final da descoberta da verdade e da justiça, todas as mais gravosas devem ser afastadas. Aqui tem-se em conta a medida proporcional que envolve o menor sacrifício para os direitos fundamentais que possam vir a ser violados. Em suma, o juízo de necessidade

[96] "As medidas de coação e de garantia patrimonial a aplicar em concreto devem ser necessárias e adequadas às exigências cautelares que o caso requerer e proporcionais à gravidade do crime e às sanções que previsivelmente venham a ser aplicadas.".

[97] "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição.".

ficará preenchido sempre que a medida seja necessária ou imprescindível para isso. Isto é, que não existam outras medidas menos gravosas que, sem impor qualquer tipo de sacrifício ou um menor grau de sacrifício, aos direitos fundamentais, tenham igualmente capacidade para atingir a aspiração da investigação criminal.

O princípio da proporcionalidade em sentido estrito é a ultima ideia fundamental que apresentamos. Aqui, o que interessa é a existência de uma ponderação entre os interesses individuais, que se vão violentar e os interesses públicos que se pretendem defender. É assim, uma ponderação entre o meio e fim pretendido. A restrição dos direitos apenas cumprirá os requisitos deste princípio, se for ponderada e equilibrada. Assim, fica proibida qualquer oneração do lesado, com uma medida que representa para este, mais prejuízo, do que as vantagens que advém para a comunidade em geral e a defesa dos interesses desta. Por outro lado, o método oculto de obtenção de prova será considerado proporcional quando o interesse público, da descoberta da verdade e da realização da justiça penal, se sobrepuser e prevalecer sobre os direitos individuais.

Direitos que não estão ligados à integridade física ou moral da pessoa, aqueles que não estão diretamente conectados com a pessoa humana, podem ser alvo de limitações e restrições. Dito isto, apesar do número 2 do artigo 18.º da CRP afirmar que pode haver restrições, quando estas forem constitucionalmente consagradas e levadas a cabo quando em concreto sejam necessárias, para salvaguardar outros interesses e direitos, também eles, constitucionalmente consagrados e apenas na medida dessa necessidade, existe um núcleo essencial de direitos, liberdades e garantias que, nunca pode ser violado e sujeito a qualquer condicionamento ou restrição.

A consagração dos métodos proibidos de obtenção de prova decorrentes do número 8 do artigo 32.º da CRP[98] são o maior exemplo do acima referido. Estes funcionam como uma verdadeira garantia da inviolabilidade dos direitos fundamentais da pessoa humana. É pois, este artigo, quando refere a intromissão abusiva nas telecomunicações como forma proibida de obter prova, que nos pode levar à conclusão que no ordenamento jurídico português, ainda não é possível o uso de *malware* como meio de obtenção de prova.

De salientar, que esta norma faz ressalva a dois planos, sendo que o primeiro, diz respeito à primeira parte da norma, às provas obtidas mediantes tortura, coação, ofensa à integridade física

[98] "São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.".

ou moral da pessoa, sendo, por consequência, sempre proibidas e por isso nulas. Já o segundo plano, que coincide com a segunda parte da norma em questão, afirma que as provas obtidas por estes métodos, apenas serão proibidas e consequentemente nulas, se a colisão se traduzir numa abusiva intromissão dos direitos fundamentais, entrando aqui em relevo o já discutido princípio da proporcionalidade em sentido amplo, e, as suas três vertentes, de forma a apurar a abusiva intromissão ou não.

Esta diferença de tratamento entre direitos, considerados ambos, fundamentais, parte da ideia que os interesses do processo penal, não poderiam acarretar nunca, um grave prejuízo para a dignidade da pessoa humana. Assim, estabeleceu-se uma proibição absoluta nos casos em que se mete em causa a dignidade pessoal. Já se admite, uma proibição relativa nos casos em que se violem outros direitos, tais como os plasmados nos artigos 26.º e 34.º, ambos da CRP.

Em suma, podemos elencar três condições de restrição de um direito fundamental. Que a sua não restritividade ameace outro direito ou interesse constitucionalmente protegido, que a Constituição expressamente preveja essa restrição, e que a restrição seja necessária para salvaguarda do direito ou interesse constitucionalmente protegido.

Consideramos, tal como Gomes Canotilho, que existem três tipos de restrições, a primeira são os limites constitucionais diretos ou imediatos, ou seja, os limites diretamente estabelecidos pela própria Constituição, a segunda são os limites estabelecidos pela lei, mediante autorização expressa da Constituição (reserva da lei restritiva) e, por fim, apresentamos os limites imanentes, ou implícitos, aqueles limites constitucionais não escritos, cuja existência é postulada pela necessidade de resolução de conflitos de bens e direitos.

O recurso à utilização, deste tipo de *software* malicioso, como método de obtenção de prova reveste um grande incremento, no que diz respeito à eficácia e à utilidade, dentro das investigações criminais em ambiente digital. As dificuldades que emergem do advento das novas formas de criminalidade, no que concerne ao combate e à prevenção do crime, impõe uma maior urgência na imposição de medidas de carácter mais gravoso, para a sua prossecução.

David Silva Ramalho[99] defende que o legislador pretendia estabelecer, através do número 2 do artigo 19.º da LC, quando se refere a "recursos a meios e dispositivos informáticos", o uso de *malware* no contexto das ações encobertas previstas no número 1 do mesmo artigo, ou seja, um novo método oculto de obtenção de provas. Segundo a sua ideia, o legislador defendia a

[99] David Silva Ramalho, "O uso de *Malware* como meio de obtenção de prova em Processo Penal", Revista de Concorrência & Regulação, (Coimbra: Almedina, 2014), pp. 195-243.

introdução de *software* malicioso no sistema informático do visado, sem o seu consentimento, para monitorizar remotamente e de forma constante, as atividades levadas a cabo por aquele sistema informático.

A nós, cabe-nos discordar, porque esta monotorização representa uma intrusão, inaceitável, ao núcleo intangível de intimidade da pessoa humana, ou seja, a colisão de direitos individuais com interesses constitucionais impõe que o legislador consagre um formalismo rígido na, possível, efetivação do recurso a este. Por isto, consideramos, que a tentativa de consagrar este meio oculto de obtenção de prova, por parte do legislador, foi feita de um modo dúbio, excessivamente vago e com um elevado défice de previsibilidade, clareza e precisão legal. Encontramos, portanto, uma violação, do número 2, do artigo 18.º e do número 1, do artigo 26.º, ambos da CRP.

Ainda, salientamos, que esta previsão foi produzida em prejuízo das garantias de defesa e do direito ao contraditório do arguido, numa área onde a prova reveste particular fragilidade. Pode, ainda, a referida norma, sofrer do vício de inconstitucionalidade, por violação do disposto nos números 1 e 5, do artigo 32.º, da CRP.

Além, de que este défice, que a norma apresenta, pode levar a interpretações diferentes, quanto aos seus requisitos e pressupostos, sendo, por isso, considerado, por nós, que o uso de *malware*, como meio de obtenção de prova, por parte dos órgãos da polícia criminal, ainda não é possível, no ordenamento jurídico português. Basta, apenas, uma melhor clareza, previsibilidade e precisão legislativa, para assim estarem cumpridos todos os requisitos necessários à utilização deste meio oculto de obtenção de prova.

5. Capítulo IV

Em alguns países, mesmo da União Europeia, já existem situações e casos em que o uso de *malware* é permitido, apesar de que com avanços, retrocessos e alguns êxitos e insucessos. Esses Estados são a Alemanha, os EUA e a Espanha. Além de que existe o Projeto HIPCAR e a Diretiva 2011/92/EU, relativamente à luta contra o abuso e a exploração sexual de crianças e a pornografia infantil (mais uma vez, crimes considerados graves, e em que o interesse e direitos públicos possam vir a ser superior aos demais direitos).

Devemos ter em conta, os instrumentos legislativos internacionais, existentes neste domínio e também tirar partido destes. Pois, podemos verificar, que as legislações nacionais de cada Estado estão cada vez mais próximas, devendo a investigação passar sempre por uma opção que vá de encontro às disposições materiais e processuais do cibercrime. E assim, regermo-nos por uma cooperação internacional que promova a troca de informação e conhecimento no seio de uma investigação, nomeadamente através de uma rede internacional que possibilite tais contactos. Consideramos, pois, que a cooperação internacional se torna imprescindível para este tipo de criminalidade.

5.1. Experiência Alemã

A experiencia alemã, no que diz respeito aos meios ocultos de investigação criminal e subsequente de obtenção de prova, diz-nos respeito, porque podemos afirmar que a jurisprudência do Tribunal Federal Constitucional alemão é como uma bússola para o nosso ordenamento jurídico. Disto é exemplo, a delineação de um núcleo essencial da conformação da vida privada como inviolável.[100]

O artigo 10.º da Constituição Alemã defende o direito a inviolabilidade da correspondência e das telecomunicações, além de que podemos encontrar uma remissão para o número 1 do artigo 2.º da mesma lei, onde se prevê o direito à privacidade.

Hoje em dia, o ordenamento jurídico alemão conseguiu reunir e consagrar os métodos ocultos de investigação criminal, como por exemplo:

[100] Rita Castanheira Neves, "As Ingerências nas Comunicações Eletrónicas em Processo Penal - Natureza e Respetivo Regime Jurídico do Correio Eletrónico enquanto Meio de Obtenção de Prova ", (Coimbra: Coimbra Editora, 2011) p.108.

- As buscas *online* que podem ser realizadas, em situações que existe perigo concreto para a vida;

- A integridade física ou a liberdade da pessoa ou para bens da comunidade, cuja ameaça afete as bases, a existência ou os fundamentos da existência do Homem[101].

Podemos ainda afirmar que se admite a vigilância de telecomunicações na fonte, ou seja, a interceção que se faz a partir do acesso, quer físico, quer através da instalação de *software*, a um sistema técnico de informações, de forma a vigiar e gravar comunicações eletrónicas em formato descodificado. [102]

No que diz respeito a meios de obtenção de prova, na investigação criminal, o ordenamento jurídico alemão, tem ao seu alcance a Lei das Telecomunicações e a Lei da Nova Regulamentação da Vigilância das Telecomunicações e outros Meios de Investigação Encoberta e da transposição da Diretiva número 2006/24/CE. Estes diplomas estabelecem as regras e os deveres de, por exemplo, as informações providenciadas pelos operadores profissionais ou sistemas fechados de comunicação.

Manuel da Costa Andrade[103] afirma que o legislador alemão, juntamente com a doutrina e a jurisprudência constitucional "tem revelado disponibilidade e capacidade para oferecer um tempestivo enquadramento normativo" nos meios ocultos de investigação. Defende ainda, que o legislador alemão tem sempre tentado erigir um verdadeiro sistema de meios ocultos de investigação criminal, nunca deixando para a lei extravagante, apesar das sucessivas alterações legislativas a consagração destes métodos, abrangendo-os sempre na StPO.

Ainda no caso alemão, o que releva é que após uma decisão do Tribunal de Justiça Federal da Alemanha, sobre um pedido de mandado judicial, para efetuar uma pesquisa remota ao sistema informático de um suspeito, instalando um *trojan*, introduziram na Lei de Proteção da Constituição da Renânia do Norte-Vestefália, uma norma que conferia à entidade responsável pela proteção da Constituição, o poder de aplicar medidas de obtenção de informação. Além de que a norma permitia, também, o acesso secreto a sistemas informáticos, instalando *malware* de forma à autoridade poder, por exemplo, monitorizar e analisar os conteúdos do sistema em causa. O Tribunal Constitucional Federal considerou que esta norma violava princípios fundamentais, tais como o direito à privacidade da correspondência e das telecomunicações e, ainda, o direito à

[101] Aresto de 27 de Fevereiro de 2008, Tribunal Constitucional Federal da Alemanha.
[102] Parte da doutrina e da jurisprudência alemã, defendem que a vigilância na fonte está ancorada pelo § 100 a. da StPO.
[103] Manuel da Costa Andrade "Bruscamente no Verão Passado...", p. 24.

autodeterminação informacional. Veio-se a concluir que a norma era inconstitucional, e que violava ainda os direitos da clareza, certeza legal e da proporcionalidade.

Pela mão do *Bundersverfassungsgericht*, contudo, assiste-se a um sancionamento e censuras reiteradas do uso de métodos ocultos de investigação criminal, em nome do princípio da proporcionalidade que fundamenta e legitima toda e qualquer restrição (e ação criminal lesiva) dos direitos fundamentais.

5.2. Doutrina e Jurisprudência Espanhola

Já na situação espanhola, podemos afirmar que a legislação específica sobre este tema é inexistente. Não é pacífico, porém, doutrinalmente, a inadmissibilidade do uso de *malware*. Existem alguns acórdãos do Supremo Tribunal Espanhol[104], que ancorados pelo artigo 22º da Lei Orgânica 15/1999, de 13 de dezembro, sobre a proteção de dados pessoais, dão autorização à utilização de dispositivos eletrónicos destinados a obter a localização física aproximada, o número IMSI e ainda o número de telemóvel que se lhe encontra associado. Segundo, Pradillo[105] a recolha destes dados pode dar abertura para o uso de formas de obter dados pessoais, em redes *wi-fi* abertas, recorrendo a *spyware*, ou seja, *malware*.

Este artigo defende que não se prevê a necessidade de precedência de mandato judicial para a aplicação do meio de obtenção de prova (recolha e tratamento de dados pessoais). Assim, podemos confrontar o regime do artigo em questão, que é jurisprudencialmente aplicado à recolha deste tipo de dados, com o regime que regula a petição de cessão dos mesmos dados às operadoras, presente na Lei n.º 25/2007, de 18 de outubro[106], no qual se consagra a obrigação de precedência de mandato judicial, constatando que, a decorrência do entendimento do Supremo Tribunal é que a autorização judicial não será exigível quando os OPC possam *motu proprio*, obter estes dados. Por outro lado, será legalmente imposta, quando os OPC precisem de ajuda das operadoras telefónicas, ou de telecomunicações para obter tais dados.[107]

Criticamos a tendência da jurisprudência, tal como David Silva Ramalho, no seu artigo denominado "O uso de *malware* como meio de obtenção de prova", em se substituir o legislador

[104] RJ 2008/4387, de 20 de Maio; RJ 2009/2089, de 18 de novembro e RJ 2009/3299, de 28 de janeiro.

[105] Apud David Silva Ramalho, "O uso de *Malware*...".

[106] Lei esta que regula a conservação de dados relativos a comunicações eletrónicas e às redes públicas de comunicações.

[107] Juan Carlos Ortiz Padrillo, "*Hacking' legal al servicio de la investigácion criminal: nuevos instrumentos para la investigación y prueba de la delinquência informática*", Delincuencia Informática. Tiempos de Cautela y Amparo, (Navarra: Thomson Teuters Aranzadi, 2012), páginas 187-191.

e na busca que esta tem, de uma interpretação que procure legitimar o uso de *malware* nos métodos de obtenção de prova existentes na *Ley de Enjuiciamento Criminal* (LEC), embora a jurisprudência espanhola venha, como os acórdãos que referimos, a interpretar certas normas no sentido de fundamentarem a admissibilidade da utilização de *malware*, em violação das exigências mínimas da legalidade e clareza estabelecidas pelo TEDH.

Como no ordenamento jurídico português, sustenta-se, e é defendido por vários autores, tais como Padrillo, que devem ser jurisprudencialmente fixados certos requisitos, para a utilização deste meio oculto de obtenção de prova. Seriam estes:

- A obrigatoriedade de precedência de mandato judicial;

- A imposição do carácter secreto da aplicação da medida;

- O estabelecimento de uma obrigatoriedade de cooperação de terceiros, especialmente das operadoras de telecomunicações quando tal se verifique ser necessário;

- O dever de fundamentação da decisão judicial;

- A excecionalidade da medida e respetiva aplicação apenas a crimes considerados graves;

- Por fim, a recolha de modo a assegurar a autenticidade e integridade da informação obtida.

Contudo, podemos afirmar que a via seguida pelo ordenamento jurídico espanhol foi outra.

O projeto *Gallardón*, vem apresentar uma profunda reforma ao nível processual e levar à aprovação de um novo Código de Processo Penal, onde no artigo 350.º se consagra, mediante prévia autorização judicial, "a utilização de dados de identificação e códigos, assim com a instalação de um *software*, que permitam, de forma remota e telemática, o exame à distancia e sem conhecimento do seu titular ou do utilizador do conteúdo de um sistema informático, dispositivo eletrónico, sistema informático, instrumento de armazenamento em massa de dados informático ou base de dados, sempre que a medida resulta proporcionada para a investigação de um delito de especial gravidade e seja ademais idónea e necessária para o esclarecimento do facto investigada, a averiguação do seu autor ou a localização do seu paradeiro."[108]

O regime previsto por este artigo e todo o novo Título XI, sobre os registos remotos sobre equipamentos informáticos, aparenta cumprir os requisitos, que nós, e também Ortiz Padrillo, consideramos obrigatórios, necessários à utilização deste tipo de meios de obtenção de prova.

[108] Apud David Silva Ramalho, "O uso de *Malware*....", página 222.

5.3 Caso dos EUA

A conferência RSA[109] em São Francisco, E.U.A., que contou com mais de 20 mil participantes teve como objetivo melhorar a proteção das empresas contra os ataques provenientes do cibercrime, tendo o diretor do FBI afirmado que, existem dois tipos de empresas, as que já foram atacadas e as que vão ser atacadas. Face a esta realidade aconselhou a que, aquelas apostem fortemente nos seus sistemas de segurança de rede e informação.

Um programa de partilha de informação – *InfraGard* – derivado de uma parceria com o sector privado, tem melhorado a segurança informática com redução de custos. O Diretor do FBI, Robert Mueller, salienta que as empresas, que são alvos de ataques informáticos, não devem ter receio de os reportar às autoridades, pois estas vão conduzir as investigações sempre com respeito pela privacidade das entidades e vítimas. Defende que uma das formas de combate ao cibercrime passa por uma partilha de conhecimento, informação e formação sobre as novas tecnologias, algo que foi instituído no seio da organização com a criação de salas de reuniões virtuais onde os investigadores analisam e partilham dados sobre os seus casos.

O responsável pela *Serious Organised Crime Agency* (Soca) - organização britânica, afirma que uma das formas de combater o cibercrime é através das empresas responsáveis pelo registo de domínios de *sites*, que devem dotar os seus sistemas atuais de ferramentas capazes de identificar quem regista domínios *web*, que depois são utilizados nestas práticas ilícitas, afirmando que "o que estamos a tentar fazer é incentivar a indústria a introduzir sistemas mais seguros, para que eles [as empresas de registo de domínios] possam saber quem é que registou estes *sites*, tenham uma base de dados de clientes mais abrangente e façam mais para evitar que os criminosos comprem *sites* e os utilizem para fins criminosos".

Já, no que diz respeito, à experiencia norte-americana na utilização de *malware* como meio de obtenção de prova, podemos caracterizá-la por atribulada, visto que, têm sido diversas as revelações do uso, não autorizado e secreto, destas medidas, por parte dos OPC. Cabe-nos dar o exemplo de duas destas situações. A primeira, que nos chama a atenção, é sobre o uso de *keyloggers* pelos OPC. Em janeiro de 1999, de forma a conseguir obter a chave que poderia decifrar dados relativos a ficheiros, suspeitos e que poderiam revestir elevado valor probatório, de forma que tais provas, poderiam ser usadas contra Nicodemo S. Scarfo, um conhecido membro de uma organização criminosa. Sendo assim, e devido a necessidade de obtenção daqueles

[109] Empresa dedicada à criptografia, que realiza anualmente uma conferência dedicada à segurança de sistemas informáticos. O seu nome resulta da junção da primeira letra do apelido dos 3 fundadores – Ron Rivest, Adi Shamier e Len Adleman, integrando o Instituto MIT.

ficheiros, o FBI solicitou um mandato judicial, para introduzir um *keylogger*, diretamente no sistema informático do suspeito, capaz de captar a palavra passe/chave necessária e de a enviar por ondas de radio para o FBI.

A segunda situação, que achamos oportuna referir, diz respeito ao *Magic Lantern*, outro tipo de *keylogger* que surgiu em 2001 e poderia ser instalado, sub-reptícia e remotamente, via Internet num sistema informático. Mais tarde, este viria dar lugar ao *Computer and Internet Protocol Adress Verifier* (CIPAV), um tipo de *malware* que juntava à lista de informações recolhidas, entre outras, o endereço IP do suspeito e a respetiva localização. Este último foi divulgado em 2007. Porém, já em abril de 2011, na sequência de um pedido submetido pela *Eletronic Frontier Foundation* ao abrigo do *Freedom of Information Act*[110], o FBI veio a divulgar vários documentos com informações detalhadas sobre o funcionamento, o enquadramento legal e a utilização do CIPAV.

Apesar de a divulgação destas duas situações ter um grande impacto no que diz respeito ao uso de *malware* como meio de obtenção de prova, este uso continua a ser feito. Prova disso é o facto de, em abril de 2013, ter sido tornada pública uma ordem judicial, subscrita pelo Juiz Stephen Smith, na qual foi negada autorização judicial para a utilização de um tipo de *malware*, não identificado, no âmbito de uma investigação criminal.[111]

5.4. União Europeia (Projeto HIPCAR e a Diretiva 2011/92/EU do parlamento Europeu e do Conselho)

No seio da U.E., podemos indicar a adoção de vários instrumentos jurídicos e programas de ação, no sentido de combate à cibercriminalidade e, todas as condutas ilícitas que daí advêm. Assim, elencamos, em primeiro lugar, a decisão n.º 1151/2003/CE do Parlamento Europeu e do conselho de 16 de junho de 2003 que altera a Decisão n.º 276/1999/CE e que adota um plano de ação comunitário plurianual, para fomentar uma utilização mais segura da internet, através do combate aos conteúdos ilegais e lesivos nas redes mundiais. A Comissão elaborou, ainda, uma Comunicação, "Europe2002, Criar uma Sociedade da Informação mais segura reforçando a segurança das infraestruturas de informação e lutando contra a cibercriminalidade",[112] sendo que

[110] https://www.wired.com/images_blogs/threatlevel/files/timberline_affidavit.pdf [consultado a 3/10/2107].

[111] Decisão disponível em: http://pt.scribd.com/doc/137842124/Texas-Order-Denying-Warrant [consultado a 3/10/2017].

[112] COM (2000) 890, Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões, intitulada "Criar uma Sociedade da Informação mais segura reforçando a segurança das infraestruturas de informação e lutando contra a cibercriminalidade".

esta, tinha em vista analisar as varias ações complementares a realizar pela U.E. para combater a cibercriminalidade. Por outro lado, devemos, ainda, apontar a Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa aos ataques contra os sistemas de informação e a Proposta de Diretiva do Parlamento Europeu e do Conselho, relativa à conservação de dados tratados no contexto da oferta de serviços de comunicações eletrónicas, publicamente disponíveis, que viria desembocar na Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006.[113]

Uma das causas que apresentámos, para a dificuldade que existe em obter-se prova no caso de ilícitos criminais informáticos, é a situação em que o Estado, no qual o visado (normalmente o que cometeu certo crime) atua, pode não ser o Estado, no qual o resultado típico se produz. E, uma vez que a aplicação dos meios de obtenção de prova continua, pelo menos na sua maioria, limitada pelo princípio da territorialidade da aplicação da lei processual penal, existe, pois, todo um interesse em que os instrumentos de investigação criminal tidos, como mais eficazes, se encontrem consagrados no maior número possível de Estados, e de forma uniforme.

Desde esta ideia, e mais precisamente a Convenção sobre o Cibercrime, de 23 de novembro de 2001, surgiu a ideia de iniciativas de cariz supranacional a nível da EU que visam promover a adoção do recurso ao *malware* como meio de obtenção de prova em ambiente digital. Assim, em dezembro de 2008, a Comissão Europeia e a ITU[114] lançaram o projeto *Harmonization of ICT Policies, Legislation and Regulatory. Procedures in the Caribbean* (HIPCAR) com o propósito de fomentar a uniformização da legislação nos países da Comunidade das Caraíbas[115] em nove áreas relacionadas com tecnologias de informação. Sendo estas áreas, transações eletrónicas, prova digital no comércio eletrónico, privacidade e proteção de dados, interceção de comunicações, cibercrime, acesso a informação pública, serviço e acesso universal, interconexão e acesso, e, por fim, licenciamento.

O artigo 27.º do *Cybercrime/e.Crimes Model Peolicy Guideliknes in Legislative Texts* prevê, como norma, o uso de *malware* em sede de investigação criminal. Claro está, e como já referimos outras vezes, no que diz respeito ao carácter intrusivo dos meios ocultos de obtenção de prova, é necessário cumprirem-se certos requisitos, tais como a exigência de que a prova não possa ser obtida de outra forma, a necessidade de precedência de autorização por parte de um juiz ou

[113] Esta diretiva, é referente à conservação de dados gerados ou trabalhados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 200/58/CE.

[114] *International Telecommunication Union*

[115] CARICOM, da qual fazem parte Antígua e Barbuda, Bahamas, Barbados, Belize, Domínica, República Dominicana, Grenada, Guiana, Haiti, Jamaica, Monserrate, Santa Lúcia, São Cristóvão e Neces, São Vicente e Grenadinas, Suriname e Trindade e Tobago.

magistrado, a exigência de densificação da autorização, concedida e ainda a limitação do seu âmbito de aplicação.

Já no lado da União Europeia, esta tem tentado fomentar a consagração deste meio de obtenção de prova. O artigo 27.º da Diretiva 2011/92/EU do Parlamento Europeu e do Conselho, relativa à luta contra o abuso sexual e a exploração sexual das crianças e a pornografia infantil, faz a seguinte consagração: " [o] s responsáveis pela investigação e pela ação penal relativas aos crimes referidos na presente diretiva deverão dispor de instrumentos de investigação eficazes. Estes instrumentos podem incluir a interceção de comunicações, a vigilância discreta, inclusive por meios eletrónicos, a monotorização de contas bancarias ou outras investigações financeiras, tendo em conta, nomeadamente, o princípio da proporcionalidade e da natureza e gravidade dos crimes investigados".

6. Conclusão

Em jeito de conclusão, sintetizamos se é ou não possível, hoje em dia, no ordenamento jurídico português a utilização por parte dos órgãos de polícia criminal o uso de *malware*, como meio de obtenção de prova.

Consideramos que não e passamos a explicar:

- Em primeiro lugar, é preciso ter em conta, a potencial lesão do uso de *malware* quando confrontado com as garantias processuais dos visados e as finalidades do processo penal, nomeadamente a intrusão desproporcional na reserva de intimidade e da vida privada. Apesar da lei, permitir alguns meios ocultos de obtenção de prova digital, tais como as ações encobertas[116], estes tem de ser efetuados, dentro das finalidades perseguidas (prevenção e repressão da criminalidade grave ou/e organizada), tem de observar os requisitos de admissibilidade e validade traçados pelo legislador, necessários à salvaguarda de outros direitos ou interesses constitucionalmente protegidos.

- Em segundo lugar, a própria CRP, também permite o recurso aos meio necessários, para garantir a realização e defesa dos direitos ou interesses protegidos, como podemos ver nos números 2 e 3 do artigo 18.º, no número 1 do artigo 25.º, no número 1 do artigo 27.º e ainda no artigo 64.º, todos da CRP.

- Em terceiro lugar, parece-nos, tal como a David Ramalho, que o legislador, com o intuito de consagrar o recurso ao *malware*, consagrou o recurso, no número 2, do artigo 19.º, da Lei do Cibercrime, a "meios e dispositivos informáticos" no contexto de ações encoberta em ambiente digital.

Mais uma vez, repetimos que para os órgãos de investigação criminal, na situação em concreto os OPC, fazerem uso de meios de obtenção de prova, devem estar cumpridos os requisitos de adequação à prossecução dos fins visados (sejam eles a prevenção ou a investigação), tem de ser necessário o uso de tal meio, sendo que o método de obtenção de prova mais eficaz e menos lesivo para os direitos que, possivelmente, virão a ser violados, é o que vai ser utilizado e por fim a proporcionalidade, assim como meio restritivo de direitos, liberdades e garantias, os métodos ocultos de obtenção de prova devem ter uma relação de justa proporcionalidade, com os fins visados pela investigação criminal e também, pela prevenção.

[116] Previstas no artigo 19.º da LC e na Lei n.º 101/2001, de 25 de agosto.

A utilização de *malware*, como meio de obtenção de provas, tal como todos os meios ocultos de obtenção de prova (mesmo os permitidos por lei), viola certo tipos de direitos processuais, além dos constitucionais já referidos, tais como, o direito a recusar testemunho ou depoimento[117] e também o direito ao silêncio[118]. Apresentamos, aqui, mais uma razão, para este método oculto de obtenção de prova não poder ser utilizado, hoje em dia, na esfera jurídica portuguesa.

O uso de métodos ocultos de investigação criminal e subsequente de obtenção de prova, mesmo o aparentemente menos ofensivo, provoca um alastramento, multiplicação e ampliação, em varias frentes dos efeitos nocivos e limitadores do núcleo essencial dos direitos fundamentais envolvidos, e por isso mesmo a existência de tantos requisitos para a utilização destes, apesar da aceitação da nossa jurisprudência de tais meios.[119]

Na nossa opinião, para estarmos perante a utilização de *malware* por parte dos órgãos de polícia criminal como meio de obtenção de prova, deveriam verificar-se uma certas mudanças e ajustamentos, principalmente no ordenamento jurídico português. Embora, possamos afirmar que a investigação de certos crimes, tais como os elencados na Lei das Ações Encobertas no artigo 19.º da LC referente à mesma matéria, poderia ser objeto da utilização deste meio de obtenção de prova, por se nos afigurar que cumprem os requisitos *supra* citados[120].Contudo, um desses não se encontra observado, que é a necessária plasmação na legislação, ou seja, o princípio da reserva da lei.

Já, no que diz respeito, ao ordenamento jurídico português achamos que o modo dúbio como o legislador consagrou o artigo 19.º n.º 2, da Lei do Cibercrime, sendo este excessivamente vago e com um elevado défice de clareza, previsibilidade e precisão legal, leva esta norma a violar o disposto dos artigos 18.º, n.º 2 e o 26.º, n.º 2 da CRP. Permitindo, assim, interpretações distintas quanto aos requisitos e pressupostos necessários para a utilização de *malware* como meio de obtenção de prova e proporcionando que a utilização deste método seja omitido nos autos ou mesmo, em geral, do conhecimento público. Além de que, prejudica as garantias de defesa e do direito ao contraditório do arguido, numa matéria onde a prova reveste particular fragilidade, podendo a norma sofrer do vício de inconstitucionalidade, por nesta situação violar o artigo 32.º, números 1 e 5, também ele da CRP.

---

[117] Artigos 134.º e 135.º, do CPP.
[118] Artigo 61.º, n.º1, alínea d), do CPP.
[119] Benjamin Silva Rodrigues, "Prova penal tomo II..." pág. 44.
[120] Páginas 37 e ss. desta dissertação.

Deixamos apenas uma ressalva, que em face da crescente popularidade que o uso de *malware* como meio de obtenção de prova, tem vindo a ganhar, e tendo em conta as suas óbvias vantagens, cremos que a tendência será a de se verificar, nos próximos anos, um esforço acrescido, pelos ordenamentos jurídicos dos Estados, principalmente nos Estados Membros da União Europeia, no sentido da sua consagração, não só no que diz respeito ao combate ao abuso sexual e exploração sexual de crianças e pornografia infantil, mas também quanto a outros tipos de criminalidade grave, tais como o terrorismo.[121]

Por fim, para uma consagração correta de um meio de obtenção de prova tão insidioso e que restringe gravemente direitos e interesses considerados fundamentais do visado, deve o legislador, prever, de forma, o mais possível, transparente, clara e suficientemente densificada os pressupostos, requisitos e finalidades da instalação e utilização de *malware* como meio de obtenção de prova em processo penal.

[121] David Silva Ramalho, "O uso de Malware..." página 225.

Bibliografia

1. ABEL, Wiebke & SCHAFER, Burkhard

   2009 "*The German Constitutional Court on the Right in Confidentiality anda Integrity of Information Technology Systems – a casa reporto n BVerfG, NJW 2008, 822*" SCRIPTed – A Journal of Law, Technology & Society, Vol. 6 nº1, pp. 106-123

2. ABREU, Carlos Pinto

3. "Prova e meios de obtenção de prova – os exames no processo penal", disponível em:

   http://carlospintodeabreu.com/public/files/CPA_prova_meios_obtencao_prova.pdf

4. ALBUQUERQUE, Paulo Pinto de

   2011 Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, 4.ª edição, Lisboa: Universidade Católica Editora

5. ANDRADE, Manuel da Costa

   1992 "Sobre as Proibições de Prova em Processo Penal", Coimbra: Coimbra Editora

   2009 a) "Bruscamente no Verão passado" a Reforma do Código de Processo Penal – Observações Criticas sobre uma Lei que Podia e Devia ter sido Diferente, Coimbra: Coimbra Editora

   2009 b) "Métodos ocultos de investigação (Plädoyer para uma teoria geral), Que Futuro para o Direito Processual Penal? Simpósio em Homenagem a Jorge Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português", Coimbra: Coimbra Editora, pp. 525-551

   2013 Sobre as proibições de prova em processo penal, Coimbra: Coimbra Editora

6. ANTUNES, Maria João

   2017 Direito Processual Penal, Reimpressão da 1.ª Edição, Coimbra: Almedina

7. AQUILINA, James M., CASEY, Eoghan & MALIN, Cameron H.

   2008 *Malware Forensics: Investigating and Analyzing Malicious Code*, EUA: Elsevier

8. AYCOCK, John

2007 *Computer Viruses and Malware*, EUA: Springer

9. BICKFORD, Jeffrey, et al.

2010 "*Rootkits on Smart Phones: Attacks, Implications and Opportunities*", Proceedings of the 11th International Workshop on Mobile Computing Systems ans Applicationas, Annapolis, Maryland, pp. 49-54

10. BOLDT, Martin

2010 *Privacy-Invasive*, Karlskrona: Blekinge Institue of Technology

11. BRENNER, Susan W., CARRIER, Brian & HENNIGER, Jef

2004 "*The Trojan horse defense in cybercrime cases*", Santa Clara Computer and High Technology Journal, Volume 24, pp. 1-53

12. CARVALHO, Paula Marques

2017 Manual Prático de Processo Penal, 10.ª edição, Coimbra: Almedina

13. CASEY, Eoghan

2011 *Digital Evidence and Computer Crime, Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet*, 3.ª edição, Califórnia: Elsevier

14. CASTRO, Catarina Sarmento

2005 Direito da Informática, Privacidade e Dados Pessoais, Coimbra: Almedina

15. CLOUGH, Jonathan

2010 *Principles of Cybercrime*, Cambridge: Cambridge University Press

16. CORREIA, Miguel Pupo & Sousa, Paulo Jorge

2010 Segurança no *Software*, Lisboa: FCA – Editora da Informática

17. DAVIS, Michael, BODMER, Sean & LEMASTERS, Aaron

2010 *Hacking Exposed – Malware & Rootkits: Malware & Rootkits & Secret Solutions*, EUA: McGraw-Hill

18. DIAS, Jorge Figueiredo

2004 Clássicos Jurídicos - Direito Processual Penal, Coimbra: Coimbra Editora

19. ERBSCHLOE, Michael

2005 *Trojans, Worms and Spyware – A Computer Security Professional's Guide to Malicious Code*, EUA: Elsevier

20. FERREIRA, Manuel Cavaleiro de,

2010 Lições de Direito Penal - Parte Geral I – II, Coimbra: Almedina

21. MARQUES, Ferreira

1988 Meios de Prova, In: Jornadas de direito processual penal. O novo código de processo penal. - Coimbra: Almedina, - pp. 219-270

22. FILIOL, Eric

2005 *Computer viruse: from theory to applications*, França: Springer

23. GONÇALVES, Fernando e ALVES, Manuel João

2009 A prova do crime – meios legais para a sua obtenção, Coimbra: Almedina

24. JESUS, Francisco Marcolina

2015 Os meios de obtenção de prova em processo penal, Verbo Jurídico

25. JOBLING, Carla e FIGUEIRA, Luís

2015 CPP Anotado - Volume II, JurIndex3, disponível em: http://www.advogados-carlajobling.pt/codigosanotados/CPP%20Anotado%20Vol%202.pdf

26. LANDAU, Susan

2010 *Surveillance or Security – The risks Posed by new Wiretapping Technologies*, EUA: MIT Press

27. MATA-MOUROS, Maria de Fátima

2011 Juiz das Liberdades – Desconstrução de um Mito do Processo Penal, Coimbra: Almedina

28. MARQUES, Garcia e MARTINS, Lourenço

2006 Direito da Informática, 2.ª Edição, Coimbra: Almedina

29. MARQUES, Maria Joana

2014 Os meios de obtenção de prova na lei do cibercrime e o seu confronto com o Código de Processo Penal, Dissertação de Mestrado

30. MCAFEE

2006 *Rootkits, Part 1 of 3: The Growing Threat*, White Paper

31. MENDES, Paulo de Sousa

2013 Lições de Direito Processual Penal, Coimbra: Almedina

32. MESQUITA, Paulo Dá

2010 Processo Penal, Prova e Sistema Juciário, Coimbra: Wolters Kluwer

33. MILITÃO, Renato Lopes

2015 A propósito da prova digital no processo penal, revista da ordem dos advogados, pp. 247-285, Lisboa

34. MOHAY, George, et al.

2003 *Computer and Intrusion Forensics*, Massachusetts: Artech House, Inc

35. MONIZ, Helena

2015 "Natureza jurídico-penal da inserção de perfis de condenados na base de dados de perfis de ADN português", comunicação apresentada nas Conferencias "A base de dados de perfis de ADN face ao direito penal e processual penal e à CEDH", Lisboa

36. MORTON, K. F. & GRACE, David

2012 "*A Case of Study on Stuxnet and Flame Malware*", disponível em: http://Vixra.org/pdf/1209.0040v1.pdf

37. NEVES, Rita Castanheira

2011 "As Ingerências nas Comunicações Eletrónicas em Processo Penal - Natureza e Respetivo Regime Jurídico do Correio Eletrónico enquanto Meio de Obtenção de Prova ", Coimbra: Coimbra Editora

38. ONETO, Isabel

2005 O Agente Infiltrado - Contributo para a compreensão do regime jurídico das acções encobertas, Coimbra: Coimbra Editora

39. PADRILLO, Juan Carlos Ortiz

2009 "*Remote Forensic Software as a Tool for Investigating Cases od Terrorism*", ENAC – E-newsletter on the fight against cybercrime, n.°4, pp. 1-8

2012 "*Hacking' legal al servicio de la investigácion criminal: nuevos instrumentos para la investigación y prueba de la delinquência informática", Delincuencia Informática. Tiempos de Cautela y Amparo*, Navarra: Thomson Teuters Aranzadi, pp. 177-220

40. PEREIRA, RUI,

2004 O "agente encoberto" na ordem jurídica portuguesa, in Medidas de Combate à Criminalidade Organizada e Económico-Financeira, Centro de Estudos Judiciários, Coimbra: Coimbra Editora.

41. POULSEN, Kevin

2013 "*FBI Admits It Controlled Tor Servers Behind Mass Malware Atack*", Wired, disponível em: http://www.wire.com/threatlevel/2013/09/freedon-hosting-fbi/

42. RAMALHO, David Silva

2014 O uso de *Malware* como meio de obtenção de prova em Processo Penal, Revista de Concorrência & Regulação, pp. 195-243, Coimbra: Almedina

43. RAMOS, Armando R. Dias

2014 a) A novíssima diretiva relativa ao cibercrime, Lisboa: EDIUAL

2014 b) A prova digital em processo penal: o correio eletrónico, Lisboa: Chiado Editora

44. RODRIGUES, Benjamim Silva

2009 Direito Penal - Parte Especial - Tomo I - Direito Penal Informático-Digital, Coimbra: Coimbra Editora

2010 Da Prova Penal – Tomo II – Bruscamente... A (s) Face (s) Oculta (s) dos Métodos Ocultos de Investigação Criminal, Lisboa: Rei dos Livros

45. ROSENBACH, Marcel

2011 "*The shady pasto f Germany's Spyware*", Spiegel Online International, disponível em http://www.spiegel.de/international/germany/trojan-trouble-the-shady-past-of-germany-s-spyware-a-792276.html

46. SANTOS, Joana Tocantins

2016 Investigações Criminais Encobertas - Da evolução do Regime Jurídico das Acções Encobertas ao equilíbrio das finalidades do Processo Penal no uso do Agente Encoberto, Dissertação de Mestrado

47. SANTOS, Paulo, et al.

2008 *Cyberwar* – O Fenómeno, as tecnologias e os actores, Lisboa: FCA – Editora de Informática

48. SIKORSKI, Michael & REIKEY, William P.

2012 *Pratical Malware Analysis – The Hands-on Guide to Dissecting Malicious Software*, San Francisco: No Starch Press

49. SILVA, Germano Marques

2011 Curso de Processo Penal – II, Lisboa: Verbo

50. SILVEIRA, Maria Ana Barroso de Moura da

2016 Da Problemática da Investigação Criminal em Ambiente Digital – em especial, sobre a possiblidade de utilização de *Malware* como Meio Oculto de Obtenção de Prova

51. SIMAS, Diana Viveiros De

2014 O Cibercrime, Dissertação de Mestrado

52. SOMESH, Christodorescu, et al.

2007 A *semantics-based approach to Malware Detection*, University of Wisconsin, USA

53. SOUSA, Paulo Pinto

2010 Ações encobertas: meio enganoso de prova? Agente infiltrado e agentes provocadores: outras questões, Revista do CEJ: *Dossier* temático direito-ordenacional, p. 231-247, Coimbra: Almedina

54. VALENTE, Manuel Monteiro Guedes

2005 Dos Órgãos de Polícia Criminal - Natureza; Intervenção; Cooperação, Coimbra: Almedina

2005 Revistas e Buscas, 2.ª edição, Coimbra: Almedina

2017 Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias", Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 3, n. 2, p. 473-482, mai./ago.

55. VARELA, Antunes, *et al*.

2004 Manual de Processo Civil, Coimbra: Coimbra Editora

56. VENÂNCIO, Pedro Dias

2011 Lei do Cibercrime: Anotada e Comentado, Coimbra: Almedina

57. VERDELHO, Pedro

2003 "Cibercrime", In Direito da Sociedade da Informação – Vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra: Coimbra Editora

2004 A obtenção de prova no ambiente digital, Revista do Ministério Público, Lisboa, N.99 (Jul./Set.2004), p. 117 a 136

2009 " *Phishing* e outras formas de defraudação nas redes de comunicação". In Direito da Sociedade da Informação – Vol. VIII, Associação Portuguesa do Direito Intelectual, Coimbra: Coimbra Editora

58. ZÚQUETE, André

2013 Segurança em redes informáticas, 4.ª edição, Lisboa: FCA – Editora da Informática

Bibliografia de Jurisprudência

59. Acórdão do Supremo Tribunal de Justiça n.º 14/2014, https://dre.pt/home/-/dre/58509400/details/maximized?p_auth=yQ03xLz3
60. Acórdão TRE de 19 de Maio de 2015, Relator Maria Leonor Esteves, http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/e2974c834606ec7780257e5800393b95?OpenDocument
61. Acórdão TRE de 12 de Julho de 2012, Relator Francisco Xavier, http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/24f86ecc0a934d7780257de10056f9f6?OpenDocument
62. Acórdão TRP de 17 de Setembro de 2014, Relator Coelho Vieira, http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/5fd1df126b7ffe9880257d6600370f95?OpenDocument
63. Acórdão TRE de 7 de Abril de 2015, Relator Fernando Pina, http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/ad8068a8c8f9b3c080257e2e00356d33?OpenDocument
64. Acórdão TRP de 12 de setembro de 2012, Relator Alves Duarte, http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/877e0322acde18d080257a8300393cc6?OpenDocument
65. Acórdão TRG de 29 de março de 2011, Relator Maria José Nogueira, http://www.dgsi.pt/jtrg.nsf/c3fb530030ea1c61802568d9005cd5bb/6aa96edf91e899b2802578a00054631f?OpenDocument
66. Acórdão TRL de 24 de setembro de 2013, Relator Vieira Lamim, http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c60dfe830c97cf8980257c0000368afa?OpenDocument
67. Acórdão TRP de 3 de Abril de 2013, Relator Artur Oliveira, http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d21c6752627b971780257b4f003caa5d?OpenDocument
68. Acórdão TRG de 15 de Outubro de 2012, Relator Fernando Monterroso, http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/d7e67584752588c980257aa0004607bc?OpenDocument