NOVA SCHOOL OF LAW

TERESA DE ARAGÃO MATTA AMARAL RAPOSO

REFLEXÕES SOBRE A ADMISSIBILIDADE DE UTILIZAÇÃO DE TÉCNICAS DE *MALWARE* NO ÂMBITO DO PROCESSO PENAL PORTUGUÊS

Dissertação com vista à obtenção do grau de Mestre em Direito na especialidade de Direito Forense e Arbitragem

Orientador:

Professor Doutor Frederico de Lacerda da Costa Pinto

junho 2023

DECLARAÇÃO ANTIPLÁGIO

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas.

Tenho consciência de que a utilização de elementos alheios não identificados, constitui uma grave falta ética e disciplinar.

AGRADECIMENTOS

Gostaria desde logo de agradecer ao Professor Doutor Frederico de Lacerda da Costa Pinto, por ter aceitado a orientação do presente trabalho.

Gostaria de agradecer igualmente à minha família, amigas e ao Diogo pelo apoio que me deram ao longo deste processo.

SIGLAS E ABREVIATURAS

al. - alínea

Ac. - Acórdão

BVerfG - Bundesverfassungsgericht

cfr. - confira, conforme

cit. - citado, citada

CPP - Código de Processo Penal

CRP - Constituição da República Portuguesa

FRCP - Federal Rules of Criminal Procedure

GPS - Global Positioning System

i.e. – isto é

JIC - Juiz de instrução criminal

LCC - Lei do Cibercrime

LECrim - Ley de Enjuiciamiento Criminal

MP - Ministério Público

n.º, n.ºs - número, números

OPC - Órgãos de polícia criminal

p., pp. - página, páginas

p.e. - por exemplo

proc. - processo

ss. - seguintes

StPO - Strafprozessordnung

TC - Tribunal Constitucional

TOR - The Onion Router

TRE - Tribunal da Relação de Évora

TRG - Tribunal da Relação de Guimarães

TRL - Tribunal da Relação de Lisboa

TRP - Tribunal da Relação do Porto

UE – União Europeia

Vol. - volume

CONVENÇÕES E ADVERTÊNCIAS

As citações de monografia serão feitas inicialmente por autor, título, edição (se for o caso), local de publicação, editora, data e página. Os artigos científicos serão citados por autor, título, publicação ou obra coletiva onde se inserem, data, páginas e site (se for o caso). As citações subsequentes serão efetuadas apenas com referência ao autor, título abreviado e página da obra, ou, tratando-se de artigo científico ou inserido em obra coletiva, título abreviado do artigo e página. As citações de notícias *online* serão feitas por autor, título da notícia, jornal, data e site. As citações de relatórios serão feitas por instituição, título, data e site. As citações subsequentes serão feitas por referência apenas ao título e páginas. A jurisprudência nacional será citada por tribunal, número do acórdão (no caso do TC), número de processo, data, e relator, estando disponíveis para consulta nos sites da DGSI ou do Tribunal Constitucional. As citações subsequentes serão efetuadas apenas com referência ao tribunal e número do acórdão. A jurisprudência internacional será citada por tribunal, data e processo. As citações subsequentes serão efetuadas apenas com referência ao tribunal e ao processo.

O corpo da tese, incluindo espaços e notas de rodapé, contém 181 200 caracteres.

RESUMO

Perante o progresso tecnológico e a emergência de técnicas de criptografia, os Estados são confrontados com novas dificuldades e obstáculos à investigação criminal, carecendo de novos métodos de investigação. Desta feita, começa a verificar-se, em diversos ordenamentos jurídicos, o recurso a técnicas de *malware*, as quais permitem o acesso oculto a dados armazenados em sistemas informáticos, bem como a monitorização da atividade aí desenvolvida e ainda a ativação de *hardware*. Não obstante, a utilização deste tipo de técnicas apresenta uma grande aptidão para compressão de inúmeros direitos fundamentais, quer do arguido, quer até de terceiros. Donde, a sua admissibilidade requer a ponderação entre, por um lado, o interesse na eficaz realização da justiça, e, por outro, a proteção daqueles direitos.

Ao passo que noutros países já se verifica a consagração da utilização deste tipo de técnicas, em Portugal a questão ainda dá azo a debate, sendo a abordagem adotada, no seio da doutrina, em geral, criticável. Em bom rigor, surgem na doutrina defensores da consagração legal deste tipo de técnicas ao abrigo de preceitos que preveem outros métodos de obtenção de prova. Porém, dada a complexidade do *malware*, dificilmente se escapa a juízos de inconstitucionalidade. Com efeito, e conforme defende outra parte da doutrina, a admissibilidade deste tipo de técnicas, no âmbito do processo penal, carece ainda da intervenção do legislador, a quem cabe proceder à consagração de habilitação legal expressa, clara e suficiente, adotando um regime que se adeque às concretas especificidades deste tipo de métodos, sob pena de constituir prova proibida.

ABSTRACT

In the face of technological progress and the emergence of encryption techniques, States are faced with new challenges and obstacles in criminal investigations, requiring new methods of investigation. As a result, various legal systems have resorted to the use of malware techniques, which allow hidden access to data stored on computer systems, as well as monitoring of the activity developed in those, and even the activation of hardware. However, the use of these techniques presents a great potential for compressing numerous fundamental rights, both of the accused and of third parties. Therefore, their admissibility requires a balance between the interest in effective justice, on the one hand, and the protection of those rights, on the other hand.

While in other countries the use of these techniques has already been established, in Portugal the issue is still subject to debate, and the approach taken by scholars can be questioned. Some proponents of the legal establishment of these techniques argue that they are covered by provisions that provide for other methods of obtaining evidence. However, given the complexity of malware, it is difficult to avoid conclusions of unconstitutionality of such regimes. In fact, as argued by another part of doctrine, the admissibility of these techniques in the context of criminal proceedings still requires the intervention of the legislator, who must provide for clear and sufficient legal authorization, adopting a regime that is suitable for the specific characteristics of these methods. Otherwise, the use of such techniques may constitute prohibited evidence.

INTRODUÇÃO

Numa época em que experienciamos as consequências de um desenvolvimento tecnológico caracterizado pela rapidez da mudança, constata-se que a investigação criminal é confrontada com obstáculos cuja ultrapassagem carece de técnicas que suscitam questões complexas quanto à sua admissibilidade. Em virtude de atualmente os dispositivos informáticos espelharem grande parte dos aspetos da vida de cada um, e perante a proliferação da *internet*, o progresso tecnológico tem possibilitado o desenvolvimento de técnicas de criptografia que oferecem aos utilizadores meios para proteger a sua privacidade digital. Não obstante, as mesmas são igualmente adotadas pelos cibercriminosos em virtude da sua aptidão para ocultação de dados, o que torna descomplicada a anonimização de informação relativamente à prática do crime. Confrontados com esta realidade, os Estados e respetivas autoridades de investigação criminal necessitam de novas técnicas de investigação que os coloquem em pé de igualdade face aos agentes do crime.

Nesta conjuntura, assistiu-se, no âmbito do processo penal de vários países, à crescente utilização de técnicas de *malware,* permitindo o acesso oculto aos sistemas informáticos, através da instalação sub-reptícia de um programa no sistema visado. Mediante esta instalação, pode não só ter-se acesso aos dados contidos no âmbito desse sistema (dados armazenados, não armazenados e produzidos em tempo real), como também é possível ativar a câmara e o microfone do dispositivo. Assim, dependendo daquilo para que o *software* for programado, este tipo de técnicas permite uma monitorização total da atividade desenvolvida no âmbito de um determinado sistema, materializando-se num verdadeiro modo de espionagem.

Não obstante, torna-se evidente que a admissibilidade deste tipo de técnicas no âmbito do processo penal português coloca questões complexas. Tratando-se de um método oculto e insidioso, o *malware* comprime necessariamente direitos fundamentais, tanto no plano material-substantivo, como processual, pelo que carece de previsão legal expressa, a qual dependerá da ponderação entre vários princípios constitucionais. Assim, na nossa análise debruçar-nos-emos essencialmente sobre a questão de saber se e em que termos a utilização de técnicas de *malware* são, ou deverão ser, admissíveis no âmbito da lei processual penal portuguesa.

Para tal, tratando-se de um método oculto, começaremos por introduzir a problemática dos métodos ocultos em geral no processo penal português, especialmente na sua relação com o princípio da legalidade, defendendo a inadmissibilidade de métodos ocultos atípicos, sob pena de cominação como prova proibida, nos termos do artigo 126.º, nº3 CPP e 32.º, nº8 e 34.º CRP.

No segundo capítulo, analisaremos alguns tipos de *malware* e suas características, explicitando quais as vantagens que estas técnicas podem trazer à investigação criminal, evidenciando em que medida o processo penal atual carece das mesmas. Perante esta constatação, torna-se necessário refletir sobre os direitos fundamentais atingidos, bem como o respetivo grau de lesão, percebendo se será possível, à luz dos princípios constitucionais, defender a admissibilidade deste tipo de técnicas, e em que termos. De seguida, socorremo-nos da análise do regime de alguns ordenamentos jurídicos estrangeiros que preveem a utilização de *malware,* o que nos permite retirar conclusões sobre o modo como outras legislações procederam à ponderação dos interesses entre a realização da justiça e a proteção dos direitos fundamentais.

Após a análise em geral das questões suscitadas pelo *malware* enquanto método de obtenção de prova em processo penal, no terceiro capítulo fazemos uma análise do "estado da arte" desta problemática no nosso ordenamento jurídico. Na nossa doutrina encontramos quem já se tenha pronunciado sobre a admissibilidade deste tipo de métodos de obtenção de prova. Não obstante, existem entendimentos divergentes, pelo que procedemos a uma análise detalhada e crítica daqueles que entendemos ser os mais significativos, concluindo que, por ausência de habilitação legal expressa, a utilização de técnicas de *malware* no nosso ordenamento jurídico é inadmissível, sob pena de constituir prova proibida, nos termos do artigo 126.º, nº3 CPP.

Por fim, deixamos no último capítulo uma nota crítica acerca da abordagem que a doutrina portuguesa adota no âmbito desta problemática, oferecendo o nosso entendimento sobre como se poderá analisar esta questão de uma forma mais clara e adequada. Efetivamente, ao longo deste processo, concluímos que as divergências e confusões existentes no seio da doutrina se prendem com uma compreensão pouco ampla da questão, o que poderá ter reflexos na inércia do legislador quanto à regulação destas técnicas. Donde, tentamos dar o nosso contributo para uma abordagem, em nosso entender, mais clara e adequada do problema.

1. MÉTODOS OCULTOS DE INVESTIGAÇÃO NO DIREITO PROCESSUAL PENAL PORTUGUÊS

1.1. ADMISSIBILIDADE

O recurso a métodos ocultos de investigação não configura uma prática dos anos recentes, tendo sido as suas vantagens para a investigação criminal há muito verificadas. Com efeito, encontramos na lei processual penal portuguesa a consagração de determinados métodos aquisitivos de prova ocultos[1], os quais são caracterizados pela circunstância de o visado não ter consciência de que está a ser alvo de uma medida desse caráter, continuando a «agir, interagir, a expressar-se e a comunicar de forma "inocente", fazendo ou dizendo coisas de sentido claramente auto-incriminatório (…)»[2]. A proliferação e recurso cada vez mais generalizado a este tipo de métodos explicam-se pelas evidentes vantagens que os mesmos têm na investigação criminal, perante a emergência de uma «nova fenomenologia criminal»[3]. Efetivamente, a transparência dos métodos de investigação criminal contende, em certa medida, com a eficácia da mesma, especialmente perante a globalização e progresso tecnológico que abrem portas a novas formas de cometimento de crimes, as quais ultrapassam o alcance da eficácia dos métodos abertos tradicionais[4]. Não obstante, os métodos ocultos de investigação, pela sua agravada danosidade social decorrente do seu caráter oculto, elevam a outro patamar a discussão acerca da procura de um equilíbrio entre a realização eficaz da justiça e a proteção dos direitos do arguido[5].

Sendo certo que a previsão de quaisquer meios aquisitivos de prova consubstancia uma restrição de direitos e liberdades fundamentais, revela-se evidente o modo como os métodos ocultos de investigação importam o sacrifício mais intenso de plúrimos valores fundamentais, tanto no plano material, como no plano processual[6] . O recurso a este tipo de métodos não só importa uma violação mais gravosa de direitos como a privacidade,

---

[1] Por exemplo, o regime das escutas telefónicas consagrado no artigo 187.º e ss. CPP

[2] 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, p. 105 e ss.

[3] *Ibidem*, p. 106. Cfr. HANS-JÖRG ALBRECHT, "Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos." in *Que futuro para o direito processual penal?: Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, (coord. Mário Ferreira Monte, et al.), Coimbra, Coimbra Editora, 2009, p. 727, referindo igualmente o problema perante a criminalidade organizada e transnacional

[4] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"...,* cit., p. 106.

[5] ANABELA MIRANDA RODRIGUES "Política criminal – novos desafios, velhos rumos" in *Liber Discipulorum para Jorge de Figueiredo Dias* (org. Manuel da Costa Andrade, et al.), Coimbra, Coimbra Editora, 2003, pp. 230 e 231, no sentido de que têm de se encontrar novos equilíbrios.

[6] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"*…, cit., p. 106

como também restringe, em certo grau, os direitos de defesa do arguido[7], o que altera significativamente a dinâmica natural[8] de um processo penal que se baseia numa tendencial igualdade de armas entre a acusação e a defesa, decorrente da sua matriz acusatória[9]. Donde, ao mesmo tempo que a falta de transparência deste tipo de métodos é o que os eleva a um nível de investigação mais eficaz, é igualmente aquilo que os torna mais problemáticos.

O direito processual penal visa a aplicação da lei penal no caso concreto[10], para o que tem de contar com meios previamente definidos, o que demanda do legislador a árdua tarefa de compatibilização dos interesses de realização de justiça com o respeito pelos direitos fundamentais do arguido. Nas palavras de HASSEMER, «a luta contra a criminalidade organiza-se tipicamente através da limitação de direitos fundamentais»[11], e, incumbindo ao Estado assegurar os direitos e liberdades fundamentais[12], tal impõe a consagração de um sistema processual penal eficaz[13], mas também a proteção dos direitos do arguido, e de terceiros, no âmbito desse mesmo processo penal. Por isso mesmo, arriscaríamos afirmar que todo o direito processual penal se baseia na procura de um equilíbrio ótimo entre a busca da verdade material, e a consequente realização da justiça, por um lado, e o respeito pelos direitos fundamentais do arguido, por outro, sendo que a disciplina da prova é aquela em que «mais vincadamente» se assiste a esse conflito[14].

---

[7] MANUEL DA COSTA ANDRADE, "Métodos ocultos de investigação, Plädoyer para uma teoria geral", in *Que futuro para o direito processual penal?: Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, (coord. Mário Ferreira Monte, et al.), Coimbra, Coimbra Editora, 2009, p. 536

[8] WINFRIED HASSEMER, "Processo penal e direitos fundamentais", in *Jornadas de Direito Processual Penal e Direitos Fundamentais* (coord. Maria Fernanda Palma), Coimbra, Almedina, 2004, p. 21

[9] Não ignorando a desigualdade material verificada entre a defesa e a acusação, a estrutura acusatória do processo, ainda que mitigada por um princípio de investigação, implica que, no geral, sejam dadas à acusação e à defesa as mesmas oportunidades de conformação do processo. Cfr. GERMANO MARQUES DA SILVA, *Direito Processual Penal Português – Noções gerais. Sujeitos processuais e objeto*, Vol. I, 7ª ed., Lisboa, Universidade Católica Editora, 2013, pp. 63 e 69

[10] RAÚL SOARES DA VEIGA, "O Juiz de instrução e a tutela de direitos fundamentais", in *Jornadas de Direito Processual Penal e Direitos Fundamentais* (coord. Maria Fernanda Palma), Coimbra, Almedina, 2004, p. 185

[11] WINFRIED HASSEMER, "Processo penal e direitos fundamentais", cit., p. 17

[12] J.J. GOMES CANOTILHO / VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, Volume I, 4.ª ed., Coimbra, Coimbra Editora, 2007, p. 277

[13] JORGE DE FIGUEIREDO DIAS, "O Processo Penal Português: problemas e prospetivas", in *Que futuro para o direito processual penal?: Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, (coord. Mário Ferreira Monte, et al.), Coimbra, Coimbra Editora, 2009, p. 806

[14] CLÁUDIA CRUZ SANTOS, "O direito processual penal, as suas finalidades conflituantes e alguns problemas de "burla de etiquetas", in *Estudos em Homenagem do Prof. Doutor Manuel da Costa Andrade*, vol. II, (org. José de Faria Costa, et. al), Coimbra: Boletim da Faculdade de Direito da Universidade de Coimbra, 2017, p. 815

Com efeito, a investigação criminal implica restrições a direitos fundamentais, enquanto é simultaneamente limitada pela tutela dos mesmos[15].

No que concerne à restrição de direitos fundamentais, esta obedece à disciplina do artigo 18.º, nº2 CRP, a qual impõe a ponderação dos valores fundamentais em jogo à luz do princípio da proporcionalidade. A especificidade dos métodos ocultos de obtenção de prova prende-se com a anulação, no momento da diligência, dos direitos de defesa do arguido, o que, como já explicitámos, contribui para o seu caráter mais devassador dos bens e direitos atingidos. Porém, o interesse na realização da justiça é igualmente um valor fundamental[16], e tratando-se de medidas necessárias à investigação e descoberta da verdade, poderão os direitos do arguido ceder. Entendemos que, como ponto de partida para o resto do texto, importa ter presente que, efetivamente, a utilização de métodos ocultos não se encontra, em abstrato, vedada pela CRP. Não obstante, a circunstância de terem um potencial tão lesivo deve igualmente estar sempre presente, pois que se afigura decisivo na consagração, e posterior interpretação, do respetivo regime legal.

Aquando da consagração de um método oculto de investigação, as exigências de proporcionalidade impostas pelo artigo 18.º, nº2 CRP levarão a que o regime legal obedeça a requisitos mais rígidos, nomeadamente, um catálogo de crimes e de alvos, reserva de juiz e um elevado grau de suspeita ou indispensabilidade[17]. Ademais, tendo em conta as considerações acerca das características dos meios ocultos de prova, necessário será também o respeito inabalável pelo princípio da reserva de lei[18], que desenvolveremos infra. Assim, apesar de a existência de métodos ocultos de investigação não configurar uma novidade, o progresso científico e tecnológico, dando espaço a novos tipos de criminalidade[19], faz-se também sentir no regime da prova em processo penal, ao permitir novas formas de investigação oculta, como o *malware*. Ora, o surgimento de novos métodos aquisitivos de prova sem o necessário acompanhamento legislativo coloca problemas ao nível do princípio da legalidade e do regime das proibições de prova.

---

[15] RAÚL SOARES DA VEIGA, "O Juiz de instrução…", cit., p. 185
[16] *Ibidem*
[17] MANUEL DA COSTA ANDRADE, "Métodos ocultos de investigação…", cit., pp. 545 e ss.
[18] J.J. GOMES CANOTILHO / VITAL MOREIRA, *Constituição da República…,* cit., p. 395
[19] Não só novos tipos de criminalidade, mas novos modos de execução e encobrimento do crime. Desenvolveremos infra, no capítulo 2.1.

1.2. Princípio da legalidade, proibições de prova e métodos atípicos ocultos

A problemática que se pretende abordar no presente estudo traz inevitavelmente à colação considerações sobre o princípio da legalidade da prova, plasmado no artigo 125.º CPP e sobre a (in)admissibilidade de métodos de obtenção de prova ocultos e atípicos, uma vez que, como teremos oportunidade de aprofundar mais à frente no presente texto, a utilização de *malware* se trata de um método atípico de obtenção de prova. Ora, em virtude do princípio da legalidade e da interpretação propugnada do artigo 125.º CPP, a sua admissibilidade encontra-se dependente de habilitação legal expressa. Havendo quem defenda a admissibilidade de métodos atípicos de prova, à luz do artigo 125.º CPP, em certas circunstâncias e mediante a verificação de determinados requisitos[20], o *malware* trata-se, ao mesmo tempo, de um método oculto de obtenção de prova, cuja utilização acarreta a violação de determinados direitos fundamentais (nomeadamente, a privacidade, autodeterminação informativa, e a confidencialidade e integridade dos sistemas informáticos, entre outros[21]), o que transporta o problema para o âmbito das proibições de prova, nos termos do artigo 126.º, nº3 CPP, e da restrição de direitos fundamentais, nos termos do artigo 18.º, nºs 2 e 3 CRP.

Apesar de as três questões não serem confundíveis, são indissociáveis. Isto é, o artigo 125.º CPP, sob a epígrafe "legalidade da prova" define, em nosso entender, e acompanhando aquela que consideramos ser a melhor doutrina, uma regra de *liberdade dentro da legalidade*[22]. Por seu turno, o artigo 126.º CPP regula as proibições de prova, concretizando o disposto nos artigos 32.º, nº8 e 34.º CRP, referindo nos nºs 1 e 2 as provas *absolutamente* proibidas, e no nº3 as provas *relativamente* proibidas. Por último, a disciplina da restrição de direitos fundamentais, nos termos do artigo 18.º, nºs 2 e 3 CRP, aplica-se a todas situações em que se operem restrições a direitos fundamentais, além daquelas no âmbito do processo penal. Ou seja, ainda que se trate de regulações distintas, estas matérias encontram-se intimamente ligadas. Efetivamente, o corpo do artigo 125.º

[20] Alberto Medina de Seiça, "Legalidade da prova e reconhecimentos «atípicos» em processo penal: notas à margem de jurisprudência (quase) constante", in *Liber Discipulorum para Jorge de Figueiredo Dias* (org. Manuel da Costa Andrade, et al.), Coimbra, Coimbra Editora, 2003, p.1411.
[21] Acerca dos direitos fundamentais comprimidos pela utilização de *malware*, *vide*, infra, capítulo 2.2.
[22] Maria Beatriz Brito, *Novas Tecnologias e Legalidade da Prova em Processo Penal. Natureza e enquadramento do GPS como método de obtenção de prova*, reimpressão, Coimbra, Almedina, 2020, p. 48. No mesmo sentido, a seguinte transcrição «(…) a legalidade da prova, cogente ao longo de todo o *iter* processual (…), é o "ambiente" dentro do qual atua e se limita a liberdade da prova.» de Pedro Soares de Albergaria, "Artigo 125º CPP" in *Comentário Judiciário do Código de Processo Penal*, Tomo II, 3ª ed., Coimbra, Almedina, 2019, p. 31

CPP determina que "*são admissíveis as provas que não forem proibidas por lei*" e as provas proibidas por lei são, nomeadamente, aquelas referidas no artigo 126.º CPP, pelo que a interpretação do preceituado no artigo 125.º é complementada pela norma do artigo seguinte. No entanto, nos termos do artigo 126.º, nº3 CPP (em conjugação com o artigo 34.º, nºs 2 e 4 CRP), meios de prova que acarretem a violação dos direitos mencionados no artigo serão admissíveis quando sejam precedidos de lei que os autorize. Estando em causa a restrição de direitos fundamentais, evidentemente que tal lei terá de obedecer às exigências plasmadas no artigo 18.º, nºs 2 e 3 CRP. Donde, compreende-se de que forma a problemática da utilização de *malware* como método de obtenção de prova convoca todas estas disciplinas.

Não pretendendo, no presente texto, proceder a uma análise demasiado extensiva acerca do princípio da legalidade, cingir-nos-emos àquilo que diretamente se relaciona com o tema proposto, e, avançando desde já uma breve conclusão, defendemos que os métodos ocultos de obtenção de prova, nos quais se inclui o *malware*, são aqueles que menos questões suscitam relativamente à admissibilidade da sua atipicidade, à luz do artigo 125.º CPP. Isto é, conforme referimos supra, por imposição constitucional, qualquer restrição a direitos fundamentais está sujeita a reserva de lei, e por isso entendemos que as questões suscitadas acerca da admissibilidade de meios de prova atípicos perdem alguma pertinência quando nos encontramos na sede dos métodos ocultos de obtenção de prova. Passemos a explicar.

A letra do artigo 125.º CPP, se não for acompanhada por um esforço de interpretação baseado no elemento teleológico da norma, nada de especial prevê. Ou seja, sob pena de se tratar de uma norma com uma previsão algo redundante uma vez que jamais se consideraria as provas proibidas por lei (artigo 126.º CPP) admissíveis[23], cabe ao intérprete atribuir-lhe um significado mais profundo, tendo sido um tal esforço de densificação já levado a cabo pela doutrina. No geral, aceita-se que a liberdade da prova implica que a prova de determinado facto não esteja prévia e legalmente vinculada a um determinado meio de prova[24]. Por outro lado, verifica-se uma corrente maioritária que defende que uma segunda vertente deste princípio de liberdade de prova se traduz no facto

[23] PEDRO SOARES DE ALBERGARIA, "Artigo 125.º…", cit., p. 31
[24] SANDRA OLIVEIRA E SILVA, "Legalidade da Prova e Provas Proibidas", in *Revista Portuguesa de Ciência Criminal*, Ano 21, nº4, outubro-dezembro 2011, p. 562

de a lei não consagrar um catálogo taxativo de meios de prova[25], com base no entendimento de que «(…) a ideia que animou o legislador (…) foi a de favorecer a descoberta da verdade material, em termos tais que implicam a admissão de todos os meios de prova e meios de obtenção dela, *ainda que não previstos na lei.*»[26]. Perante um tal entendimento, afigura-se necessário traçar os limites daquilo que é admissível à luz do artigo 125.º CPP, em relação àquilo que se encontra vedado pelo princípio da legalidade. Em bom rigor, o princípio da descoberta da verdade material não é absoluto e o regime legal traçado pelo legislador para os meios de prova típicos não pode ser subalternizado a qualquer custo em nome da verdade material. Um entendimento contrário levar-nos-ia a questionar, então, por que razão teria o legislador consagrado um catálogo de meios de prova e métodos de obtenção de prova?

Sendo relativamente unânime que, no que concerne aos meios de prova tipificados, o intérprete se encontra adstrito ao regime legal consagrado, não podendo subalternizá-lo em função da sua vontade, pois que isso desvirtuaria a própria existência de um catálogo, a doutrina[27] tende a aceitar, em abstrato, a admissibilidade de meios atípicos, quando os mesmos sejam verdadeiramente atípicos e não se traduzam num mero desvirtuamento do regime existente, estabelecendo, desde logo, um limite à liberdade das formas aquisitivas. Assim, perante um meio aquisitivo de prova *a priori* atípico, e com base na interpretação do artigo 125.º que viemos defendendo, fundamental será verificar a ausência de um meio típico «idóneo a produzir o mesmo resultado cognoscitivo»[28]. Contudo, passado esse crivo, não cremos que se encontre automaticamente autorizado o recurso a tal método. Não podemos deixar de ter presente que o processo penal português assenta «num modelo probatório conformado pela tutela dos direitos fundamentais das pessoas (…)»[29], circunstância essa que decorre da sua matriz acusatória, assente no equilíbrio entre a busca da verdade material e o respeito pela pessoa do arguido. Donde, compreende-se que os métodos de obtenção de prova, típicos ou atípicos, se encontrem,

---

[25] ALBERTO MEDINA DE SEIÇA, "Legalidade da prova…", cit., p. 1407; PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª ed., Lisboa, Universidade Católica Editora, 2011, p. 332

[26] PEDRO SOARES DE ALBERGARIA, "Artigo 125.º…", cit., p. 37

[27] ALBERTO MEDINA DE SEIÇA, "Legalidade da prova…", cit., p. 1411; PEDRO SOARES DE ALBERGARIA, "Artigo 125.º…", cit., p. 34; PAULO DE SOUSA MENDES, "As Proibições de Prova no Processo Penal" in *Jornadas de Direito Processual Penal e Direitos Fundamentais* (coord. Maria Fernanda Palma), Coimbra, Almedina, 2004, p. 135

[28] SANDRA OLIVEIRA E SILVA, "Legalidade da Prova e Provas Proibidas", cit., p. 15

[29] ALBERTO MEDINA DE SEIÇA, "Legalidade da prova…", cit., p. 1408

necessariamente, balizados pelo artigo 126.º CPP[30]. Parecendo esta uma afirmação relativamente evidente, a prática mostrou-nos que a resolução do problema não é, no entanto, assim tão simples.

Entre nós, a admissibilidade de um método de aquisição probatória atípico restritivo de direitos fundamentais tem sido amplamente discutida na jurisprudência a propósito da utilização de aparelhos de GPS como método de obtenção de prova. Sem pretensão de levar a cabo grandes desenvolvimentos sobre essa problemática, entendemos que se afigura pertinente fazer-lhe uma referência no presente estudo, uma vez que, ao tratar-se de um método oculto atípico, levanta algumas questões de natureza semelhante àquelas que são suscitadas a propósito da utilização de *malware*. Apesar de as decisões analisadas não se debruçarem amplamente sobre a problemática de métodos ocultos atípicos, consideramos que as soluções encontradas na jurisprudência sobre a conformidade legal de aparelhos de GPS como método de obtenção de prova merecem análise em virtude de ser precisamente a sua a natureza *atípica* e *oculta* que está na origem do debate acerca da sua admissibilidade. Melhor dizendo, não se referindo, em abstrato, a admissibilidade de métodos ocultos atípicos, em todos os acórdãos analisados a problemática reside em perceber se existem normas que vislumbrem a utilização de GPS como método de obtenção de prova, e, não existindo, qual a medida de lesão de direitos fundamentais, à luz do artigo 126.º CPP, de modo a concluir ou não pela legalidade da utilização daquele aparelho, aí residindo a relevância para o presente estudo.

Em decisão de 07-10-2008[31], o TRE decidiu pela admissibilidade da utilização de aparelhos de GPS enquanto método de obtenção de prova, com base no entendimento (em nossa opinião, erróneo[32]) de que não se trata de um método atentatório da vida privada do visado, não consubstanciando, portanto, nos termos do artigo 126.º, nº3 CPP, um meio de prova nulo, sendo então permitido à luz do artigo 125.º CPP. No sentido da admissibilidade da utilização do GPS foi também o acórdão do TRP de 21-03-2013[33]. Não obstante, foi diversa a fundamentação, considerando-se que a utilização de GPS

[30] PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, cit., p. 332
[31] Ac. TRE, proc. 2005/08-1, de 07-10-2008, Rel. Martinho Cardoso
[32] Sem pretensão de extravasar o âmbito do presente estudo, acompanhamos a opinião daqueles que rejeitam a equiparação do GPS a métodos tradicionais de vigilância policial, considerando que «*(...) o carácter tecnológico/digital empresta-lhe um lastro de aplicação necessariamente mais amplo e invasivo, naturalmente decorrente da circunstância de se tratarem de dados obtidos via satélite. (...)*», cfr. MARIA BEATRIZ BRITO, *Novas tecnologias e legalidade da prova em processo penal*, cit., p. 65
[33] Ac. TRP, proc. 246/12.9TAOAZ-A.P1, de 21-03-2013, Rel. Joaquim Gomes

permite «traçar o perfil detalhado da vida pública e privada de uma pessoa (…)»[34], defendendo a aplicação analógica do artigo 187.º CPP, que regula o regime das escutas, para que a utilização de aparelhos de GPS seja sujeita a autorização judicial, em virtude da afronta sensível a direitos fundamentais. Esta solução resulta do facto de o tribunal considerar que os dados de localização podem ser obtidos tanto por dados telefónicos, como por dados obtidos por via do mecanismo de GPS, semelhança esta que justificaria o recurso à analogia. Não podemos deixar de criticar esta decisão. Sendo certo que é admissível o recurso à analogia para a integração de lacunas em processo penal (artigo 4.º CPP), o mesmo encontra-se balizado pelo disposto nos artigos 29.º, nº1 e 32.º, nº1 CRP[35], no sentido de que é proibida a analogia quando se traduza num enfraquecimento da posição do arguido ou na diminuição dos seus direitos processuais[36]. Nesta sede, seguimos de perto o ensinamento de FIGUEIREDO DIAS[37], ao salientar que também no processo penal (além do direito penal substantivo) se coloca em causa a liberdade dos cidadãos, consubstanciando o princípio da legalidade uma garantia contra eventuais arbítrios do Estado, devendo, portanto, o recurso à analogia encontrar-se vedado quando tal comporte o desfavorecimento da posição do arguido. Sendo de salientar que, no que concerne a um método de obtenção de prova oculto, o qual restringe, necessariamente, os direitos de defesa do arguido, sempre se trataria de uma analogia *in malam partem*. Por outro lado, como tivemos oportunidade de explicitar, a restrição de direitos fundamentais carece de habilitação legal expressa, nos termos do artigo 18.º, nºs 2 e 3 CRP, circunstância esta que se opõe naturalmente ao recurso à analogia[38]. O próprio tribunal reconhece, ao contrário do TRE, que se está perante um método aquisitivo que interfere com a vida íntima e o direito à autodeterminação informacional do visado, parecendo-nos que andou mal ao concluir pela aplicação analógica do artigo 187.º. Conforme clarificámos, entendemos que é inadmissível o recurso à analogia nesta sede, no sentido de ser uma afronta constitucional operar uma restrição a direitos fundamentais por via de aplicação analógica, ainda que reconheçamos que as escutas telefónicas consubstanciam

[34] Ac. TRP, proc. 246/12.9TAOAZ-A.P1, de 21-03-2013, Rel. Joaquim Gomes
[35] Cfr. Ac. TC nº 324/2013, proc. nº 87/12, Rel. Maria João Antunes
[36] MARIA JOÃO ANTUNES, *Direito Processual Penal*, 3ª ed., Coimbra, Almedina, 2021, p. 30
[37] JORGE DE FIGUEIREDO DIAS, *Direito Processual Penal*, reimpressão, Coimbra, Coimbra Editora, 2004, p. 96 e ss.
[38] MANUEL DA COSTA ANDRADE, "Métodos ocultos de investigação…", cit., p. 541

um exemplo paradigmático de métodos ocultos de obtenção de prova, com um regime exemplar[39].

Num sentido diverso, de rejeição da utilização do GPS, surge a decisão do TRL de 13-04-2016[40], que, em nossa opinião, vai no sentido mais acertado. Lê-se na fundamentação da decisão que «(…) porque um aparelho de geolocalização, no caso, um "GPS tracker", é um meio oculto de investigação que, por isso mesmo, só poderia ser admitido se existisse lei que o consagrasse como um meio de obtenção de prova legítimo e regulasse todos os referidos aspectos do seu regime». Efetivamente, e como temos vindo a desenvolver, os métodos ocultos atingem diferentes bens jurídicos e direitos fundamentais, tanto no plano material-substantivo, como no plano processual[41], pelo que se compreende que a legitimidade de recurso aos mesmos, no âmbito do processo penal no quadro de Estado de Direito, careça necessariamente de intervenção legislativa[42].

Esta breve excursão sobre algumas decisões jurisprudenciais relativas à admissibilidade de utilização de GPS como método de obtenção de prova em processo penal pretendeu evidenciar a complexidade prática desta questão. Em bom rigor, não se coloca em causa que a restrição de direitos fundamentais obedece a um princípio de reserva de lei, no entanto, o desenvolvimento tecnológico e a proliferação de possibilidades ocultas de investigação não deixam de colocar questões. Efetivamente, métodos como a utilização de GPS e a utilização de *malware* não se encontram regulados, mas apresentam vantagens indiscutíveis, tentando a jurisprudência e a doutrina socorrer-se de esforços de interpretação para defender a sua admissibilidade[43]. Nas palavras de COSTA ANDRADE, *«*outros [métodos ocultos], pura e simplesmente, não conheceram ainda sancionamento legal e vão fazendo curso na margem da ilegalidade*»*[44].

Conforme explicitámos supra, a questão coloca-se num ordenamento jurídico no qual vigora uma regra de *liberdade dentro da legalidade*. Ora, independentemente das nuances que existam nas diferentes interpretações doutrinárias do artigo 125.º CPP[45], entendemos que, aceitando em abstrato a admissibilidade de métodos atípicos de

[39] MANUEL DA COSTA ANDRADE, "Métodos ocultos de investigação…", cit., p. 533
[40] Ac. TRL, proc. 2903/11.8TACSC.L1-3, de 13-04-2016, Rel. Carlos Almeida
[41] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"…,* cit.*,* pp. 106 e ss.
[42] *Ibidem*, pp. 112 e ss.
[43] Sobre o *malware*, *vide* capítulo 3 do presente texto
[44] MANUEL DA COSTA ANDRADE, "*Bruscamente no Verão Passado"…,* cit., p. 109
[45] Não pretendendo entrar aprofundadamente no debate sobre a admissibilidade de meios de prova atípicos em processo pena, há quem rejeite totalmente tal admissibilidade.

obtenção de prova, com os limites identificados supra, dificilmente se poderá advogar a aceitação de métodos atípicos ocultos. Este tipo de métodos aquisitivos apresenta, no geral, determinadas características paradigmáticas, nomeadamente tornarem os tradicionais direitos processuais do arguido obsoletos, naturalmente, dada a sua natureza secreta; serem abrangentes e incidirem necessariamente sobre um elevado número de pessoas e gerarem várias informações, relativamente ao passado, presente ou futuro[46], o que reclama um cuidado acrescido na sua regulação. Não podemos deixar de enfatizar novamente o grau de intrusão que este tipo de métodos comporta, sendo que a primeira conclusão a retirar é a de que a admissibilidade de métodos ocultos de obtenção de prova carece de habilitação legal expressa[47], sob pena de constituir prova proibida, nos termos do artigo 126.º, nº3 CPP.

Assim, quanto aos métodos ocultos de obtenção de prova, o silêncio da lei não autoriza a prática[48] por um lado, e, por outro, a lei habilitante tem de apresentar densidade normativa suficiente[49]. É com base nesta premissa que partimos para a reflexão, em concreto, sobre a admissibilidade de utilização de técnicas de *malware* no processo penal.

[46] HANS-JÖRG ALBRECHT, "Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos.", cit., p. 726

[47] Também rejeitando a admissibilidade de métodos ocultos atípicos, JOÃO GOUVEIA CAIRES, "Métodos ocultos na criminalidade económico-financeira: entre a (a)tipicidade e a cumulação", in *JULGAR,* nº38, 2019, p. 80, disponível em: http://julgar.pt/wp-content/uploads/2019/05/JULGAR38-04-JC.pdf (consultado a 25/11/2022)

[48] MARIA BEATRIZ BRITO, *Novas tecnologias e legalidade da prova em processo penal*, cit., p. 57

[49] JOÃO GOUVEIA CAIRES, "Métodos ocultos na criminalidade económico-financeira…", cit., p. 60

2. O *MALWARE* COMO MÉTODO DE OBTENÇÃO DE PROVA

Numa época em que a utilização de várias tecnologias e o acesso à *internet* estão absolutamente consolidados no quotidiano de todos nós, assiste-se também a um aumento da utilização da *internet* e do meio digital para o cometimento de crimes. Esta conjuntura tem vindo a verificar-se e consolidar-se desde o início do século, e cedo os Estados mostraram preocupação com a adaptação do Direito à nova realidade. Em 2009 Portugal adotou um "pacote cibercrime"[50], através da ratificação da Convenção sobre Cibercrime de 2001[51] e da transposição para a ordem jurídica interna a Decisão-Quadro nº2005/222/JAI do Conselho, de 24 de fevereiro, através da Lei nº109/2009 de 15 de setembro (LCC), a qual não só, mas sobretudo, introduziu no nosso sistema jurídico novos métodos de obtenção de prova em ambiente digital[52], com o desiderato de «responder ao diagnóstico de uma carência do ordenamento jurídico nacional relativa à recolha de prova eletrónica»[53].

Efetivamente, ao tempo da entrada em vigor da LCC, já o legislador ia com algum atraso na abordagem do problema suscitado pelos avanços tecnológicos. Isto é, era premente, em virtude das novas técnicas informáticas, que o legislador adaptasse a lei processual penal às novas realidades[54]. Desde então, tem-se continuado a verificar enormes avanços tecnológicos, os quais, porém, não têm sido acompanhados pelo legislador. Por outro lado, nos últimos anos tem-se assistido a uma transformação da sociedade no geral, tendo a maioria das pessoas transportado uma parcela da sua vida para o meio digital, armazenando muita informação em sistemas informáticos[55]. Donde, o acesso aos mesmos constitui uma preocupação crescente por parte dos Estados no âmbito da investigação criminal, não só nos casos de crimes cometidos por via de sistemas informáticos, como também pela aptidão destes sistemas para guardar e gerar informação

---

[50] JOSÉ DE OLIVEIRA ACENSÃO, "O Cibercrime", separata de *Direito Penal Económico e Financeiro: conferências do curso pós-graduado de aperfeiçoamento* (coord. Maria Fernanda Palma, et al.), Coimbra, Coimbra Editora, 2012, p. 311

[51] Através de decreto do Presidente da República n.º91/09. ARMANDO DIAS RAMOS, *O Agente Encoberto Digital: meios especiais e técnicos de investigação criminal*, Coimbra, Almedina, 2022, p. 185;

[52] JOÃO CONDE CORREIA, "Prova digital: as leis que temos e as leis que devíamos ter", in *Revista do Ministério Público*, nº139, julho-setembro 2014 p. 35

[53] PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora, 2010, p. 97

[54] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"…*, cit., p. 184

[55] BENJAMIM SILVA RODRIGUES, *Da Prova Penal – Tomo II, Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010, pp. 472 e 473

que pode constituir prova fulcral[56]. Ora, acautelando a LCC, até certo ponto, a realidade da era digital em que vivemos, a lei não evolui ao ritmo da tecnologia, pois esta se encontra em constante e rápida mudança e inovação, sendo inexigível (e impossível) que a lei acompanhe o ritmo frenético do progresso tecnológico. Este tipo de avanços permite também que os agentes no ciberespaço desenvolvam técnicas que permitem contornar os tradicionais (e legalmente previstos) métodos de investigação, assistindo-se, no plano tecnológico, ao robustecimento de técnicas orientadas para a proteção da confidencialidade e integridade dos dados informáticos[57], as quais são aproveitadas pelos agentes do crime não só para o cometimento de ilícitos penais, mas também para ocultação, eliminação e modificação da prova[58]. Naturalmente, este fenómeno dificulta o acesso aos sistemas informáticos e as autoridades carecem de meios intrusivos de investigação, que, correspondendo a técnicas tradicionalmente utilizadas pelos agentes do crime, lhes permitam ter acesso a semelhantes vantagens tecnológicas[59]. De outro modo, os agentes do crime estariam sempre um passo à frente das autoridades, e afigurar-se-ia uma tarefa extremamente espinhosa (quem sabe, impossível) recolher prova em determinados ambientes informáticos. Uma das técnicas a que nos referimos é precisamente o *malware*.

Uma questão prévia a abordar prende-se com a utilização do termo *malware* por oposição a quem se refere a buscas *online*[60]. Nas palavras de MANUEL DA COSTA ANDRADE, o termo de buscas *online* trata-se de «um conceito compreensivo e abrangente, porventura mesmo não inteiramente rigoroso, a que se reconduz um conjunto de intromissões nos sistemas informáticos, feitas através da internet e que se atualizam na observação, busca, cópia, vigilância, etc., dos dados presentes naqueles sistemas

---

[56] JULIANA SOUSA CAMPOS, *O Malware como meio de obtenção da prova em processo penal*, Coimbra, Almedina, 2021, p. 32

[57] JAMES A. LEWIS / DENISE E. ZHENG / WILLIAM A. CARTER, "The effect of encryption on lawful access to communications and data" A report of the CSIS Tecnhology policy program, 2017, pp. 2 e 3, disponível em: https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data (consultado em 17/2/2023)

[58] RYAN HARRIS, "Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem", *Elsevier*, 2006, pp. 44-45, disponível em: https://www.researchgate.net/publication/222662987_Arriving_at_an_anti-forensics_consensus_Examining_how_to_define_and_control_the_anti-forensics_problem (consultado a 27/12/2022)

[59] JULIANA SOUSA CAMPOS, *O Malware…,* cit., p. 33

[60] Socorrendo-se do conceito de busca *online*, cfr. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"…*, cit., p. 166; PAULO PINTO DE ALBUQUERQUE, *Comentário ao Código de Processo Penal…*, cit., p. 502

informáticos.»[61]. Entendemos que se está perante um entendimento de busca *online* que abrange o conceito de *malware,* nas suas vertentes de instalação, pesquisa e recolha de informação[62]. De forma sucinta, entende-se que o conceito de *malware* abrange «todo o tipo de programas instalados sub-repticiamente por terceiros num sistema informático que podem ser utilizados para, de algum modo, comprometer as suas funções, contornar os seus controlos de acesso, causar prejuízo ao seu utilizador ou ao sistema informático infetado, monitorizar a sua atividade ou apropriar-se, corromper, eliminar e/ou alterar dados informáticos»[63]. De outro modo, há quem se refira ao termo *benware*, de modo a afastar-se da conotação negativa do termo *malware*[64]. Ponto é que, ainda que utilizando terminologias distintas, muita doutrina se refere à mesma realidade de infiltração oculta num sistema informático através da instalação remota de um *software*. No entanto, e de modo que não haja azo a equívocos de compreensão, na senda de DAVID SILVA RAMALHO[65] e JULIANA CAMPOS DE SOUSA[66], preferimos no presente texto adotar o conceito de «*malware»* ou a expressão «técnicas de *malware*», por entendermos que se apresenta mais adequado à análise que pretendemos levar a cabo no presente estudo. Não obstante, como teremos oportunidade de aprofundar no capítulo 4 deste texto, consideramos que esta multiplicidade de nomenclaturas se traduz também numa abordagem não totalmente adequada da problemática, ainda que reconheçamos a dificuldade em arranjar uma única terminologia que traduza rigorosamente o problema sob estudo.

Ultrapassada a questão da terminologia escolhida, procuraremos no próximo subcapítulo expor as especificidades do *malware* e as consequentes vantagens para a investigação criminal.

[61] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"...,* cit., p. 166
[62] DAVID SILVA RAMALHO, "O uso de malware como meio de obtenção de prova em processo penal", in *Revista de Concorrência e Regulação*, ano IV, nº16, outubro-dezembro, 2013, p. 199
[63] *Ibidem*, p. 202
[64] ARMANDO DIAS RAMOS, *O Agente Encoberto*…, cit. p. 208
[65] DAVID SILVA RAMALHO, "O uso de malware…", cit., pp. 199 e ss.
[66] JULIANA SOUSA CAMPOS, *O Malware...,* cit., pp. 33-34

2.1. NATUREZA E ESPECIFICIDADES DO *MALWARE* E CONTRIBUTOS PARA A INVESTIGAÇÃO CRIMINAL

O termo *malware* resulta da junção dos termos «malicious» e «software»[67], sendo caracterizado por se tratar de um *software* intrusivo e insidioso em relação ao sistema informático no qual se instala[68]. Desde logo, é de notar que o *malware* não se traduz num único programa, operando sempre de forma linear e apresentando sempre as mesmas características. Na verdade, pode assumir diversas vestes, o que se apresenta como um primeiro sinal da complexidade deste método de obtenção de prova. Por outro lado, o seu modo de instalação, ou seja, o modo através do qual se infiltrará no sistema informático do visado, também pode ocorrer com recurso a diferentes técnicas. Tendo já oferecido uma definição simultaneamente completa e sucinta de *malware*[69], começaremos agora por explicar de forma breve alguns dos tipos de instalação de *malware* a que se pode recorrer no âmbito das investigações criminais, após o que enunciaremos as principais ameaças e dificuldades com que as autoridades de investigação criminal se deparam atualmente e que justificam a necessidade de recurso ao *malware.*

No âmbito das investigações criminais, o tipo de *malware* mais comummente referido são os cavalos de Tróia[70], mas há que introduzir no debate igualmente os restantes tipos de *malware* suscetíveis de serem utilizados no âmbito de investigações criminais, em virtude da utilidade e vantagens que as suas funcionalidades podem apresentar nesse contexto[71]. Nomeadamente, seguindo DAVID SILVA RAMALHO[72], as *logic bombs*, o *spyware*, os *rootkits*, os vírus, os *worms*, e as *blended threats*. Isto sem prejuízo da existência de muitos outros tipos de técnicas de infiltração oculta em sistemas informáticos.

Os cavalos de Tróia tratam-se de um tipo de *malware* que se apresenta como algo inócuo com o intuito de levar o visado a adotar uma qualquer conduta ativa (p.e., abrindo uma página *web* infetada com um código malicioso) que resulte na instalação do programa no sistema informático pretendido[73]. Instalado o *malware* no sistema

---

[67] DAVID SILVA RAMALHO, "O uso de malware…", cit., p. 201
[68] *Ibidem*
[69] *Vide*, p. 15 do presente texto
[70] DAVID SILVA RAMALHO, *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra, Almedina, 2017, p. 319; MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão passado…",* cit., p. 165; BENJAMIM SILVA RODRIGUES, *Da Prova Penal…,* cit., p. 380
[71] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 319
[72] *Ibidem*
[73] *Ibidem,* p. 320

informático, o terceiro tem a porta aberta para recolher as mais diversas informações contidas naquele, monitorizar a atividade levada a cabo no sistema, e até navegar na *internet* enviando informação a partir do sistema infetado[74].

As *logic bombs* são definidas por ERIC FILIOL como «malware não replicativo que se instala num sistema e espera por um evento-gatilho que desencadeie uma ação ofensiva»[75]. Este autor dá o exemplo de uma *logic bomb* desenvolvida e instalada na rede de uma empresa pelo administrador dessa rede, a qual verificava todos os dias se o nome do mesmo se encontrava no registo da contabilidade da empresa. Quando o nome do administrador deixou de constar dos documentos, em virtude de ter sido despedido, a *logic bomb* cifrou todos os documentos da empresa, incluindo *back ups*, tornado os documentos indecifráveis[76]. O modo de operação deste tipo de *malware* torna-o resistente a antivírus[77].

O *spyware* trata-se de um programa informático que recolhe informação sobre uma pessoa ou organização sem o seu consentimento ou conhecimento[78]. Este *software* pode incluir programas que permitem intercetar os pacotes de dados que fluem por aquele ponto da rede (*sniffers*), ou programas que permitem gravar informações sobre as teclas premidas pelo utilizador (*keyloggers*)[79]. Este programa permite, no essencial, monitorizar a atividade do utilizador do sistema informático e transmitir informação ao atacante[80].

Os *rootkits* operam normalmente através de alguma vulnerabilidade do sistema operativo, permitindo a um intruso ganhar acesso privilegiado de administrador a um sistema informático e facilitando a instalação de outro tipo de *malware,* como aqueles já referidos, tornando-os indetetáveis a antivírus ou *anti-spyware*[81].

---

[74] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 320
[75] ERIC FILIOL, *Computer Viruses: from theory to application*, Springer, 2005, p. 99, disponível em: https://repository.root-me.org/Virologie/EN%20-%20Computer%20viruses%20from%20theory%20to%20applications.pdf (consultado a 14/12/2022). Tradução livre
[76] *Ibidem*, p. 100
[77] *Ibidem*
[78] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 321
[79] O recurso a *keyloggers* verificou-se num caso nos EUA, cerca de 1999, que ficou conhecido como um dos primeiros casos de recurso a *malware* no âmbito do processo penal. Sobre a utilização de técnicas de *malware* nos EUA, *vide* capítulo 2.3.1
[80] JULIANA SOUSA CAMPOS, *O Malware…,* cit., p.39
[81] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 321

O vírus é um tipo de *malware* desenhado para se espalhar autonomamente de dispositivo em dispositivo, danificando o sistema, corrompendo ou eliminando dados[82]. Os *worms* são semelhantes aos vírus, constituindo, porém, um *software* autónomo que se propaga através da *internet*, sem necessidade de um programa hóspede ou de interação humana para se propagarem[83].

Feita uma breve excursão sobre os tipos de *malware* que poderão ser utilizados na investigação criminal é desde logo evidente a aptidão deste tipo de técnicas para monitorização da atividade exercida num determinado sistema informático, em termos semelhantes a uma espionagem total da atividade do visado, e a recolha de dados presentes no mesmo, o que é um traço distintivo deste em relação a outros métodos de obtenção de prova previstos na nossa legislação. Por exemplo, podendo a utilização de *malware* afetar a privacidade das telecomunicações, tem em si uma vocação muito mais ampla do que aquela da "mera" intromissão nas telecomunicações. Por outro lado, permitindo a monitorização da atividade no sistema informático afetado, possibilita o acesso a dados produzidos em tempo real, e não apenas a dados já armazenados em tal sistema[84]. Assim, este método de investigação, podendo apresentar semelhanças em relação a outros que encontramos na nossa lei, tem aspetos que o singularizam e o colocam noutro patamar no contexto da afetação dos direitos fundamentais.

De igual forma, é evidente como, dependendo da programação do *software* em concreto utilizado, se permite uma panóplia de ações: no estádio atual do desenvolvimento tecnológico, as possibilidades trazidas por estas técnicas para o mundo da investigação criminal são inimagináveis. Em bom rigor, a tecnologia pode estar ao serviço daquilo que as autoridades de investigação pretenderem, e, assim, dependendo do tipo de diligência em causa, dos direitos afetados e do modo e grau dessa afetação, estaremos perante realidades distintas. Donde, sem prejuízo de retomarmos esta questão posteriormente[85], avançamos desde já a ideia de que não será a abordagem mais acertada encarar a utilização de *malware* na investigação criminal enquanto um método de prova como um todo em si, sujeito a um regime unitário.

---

[82] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 321
[83] *Ibidem*
[84] JULIANA SOUSA CAMPOS, *O Malware…,* cit., p. 87
[85] Capítulo 4 do presente texto

Apesar disto, a potencial eficácia deste método de obtenção de prova não vale por si só: como explicitámos no capítulo anterior, a investigação criminal não pode, dentro de um quadro de Estado de Direito baseado no respeito pelos direitos fundamentais dos cidadãos, ser feita a qualquer custo. Antes, e especialmente no cenário de métodos de obtenção de prova, se deve integral cumprimento do princípio da proporcionalidade nos termos do artigo 18.º, nº2 CRP. No concreto âmbito em que nos encontramos, é sobretudo relevante a vertente da exigibilidade ou necessidade, no sentido de que os fins visados pela lei, *in casu* os fins atingidos através da utilização de *malware*, não seriam obtidos por via de outros meios menos onerosos[86]. Donde, cabe aferir da sua relevância e indispensabilidade para a investigação criminal nos dias que correm.

Para tal, cumpre ter presente o surgimento e proliferação das medidas anti-forenses, que se podem caracterizar por se tratarem de métodos que comprometem a disponibilidade ou utilidade da prova, eliminando, ocultando ou até modificando dados informáticos[87] que possam constituir prova. Concretamente no que concerne à ocultação de dados, é de realçar o recurso à encriptação[88], uma vez que se encontra presente em diferentes serviços[89] e, tendo como objetivo acautelar a privacidade dos seus utilizadores na época digital em que vivemos, é porém cada vez mais utilizada pelos agentes do crime[90] com o intuito de dificultar a sua investigação. A encriptação consiste num «processo de transformação de informação num formato seguro para a proteger do acesso não autorizado de terceiros»[91]. De forma simplificada, a encriptação funciona através da utilização de uma ou mais chaves, só tendo acesso ao conteúdo da informação quem

---

[86] J.J. GOMES CANOTILHO / VITAL MOREIRA, *Constituição da República…,* cit.*,* p. 393

[87] RYAN HARRIS, "Arriving at an anti-forensics consensus…" cit., p. 44

[88] KEVIN CONLAN / IBRAHIM BAGGILI / FRANK BREITINGER, "Anti-forensics; furthering digital forensic science through a new extended, granular, taxonomy", *Elsevier*, 2016, p. 71, disponível em: https://www.sciencedirect.com/science/article/pii/S1742287616300378 (consultado a 14/2/2023)

[89] Nomeadamente, aplicações de troca de mensagens como *WhatsApp*, *Facebook Messenger*, *Signal*, *Telegram.* Cfr. EUROPOL/EUROJUST, "First report of the observatory function on encryption", janeiro de 2019, p. 15, disponível em: https://www.eurojust.europa.eu/news/first-europoleurojust-report-encryption-observatory-function#:~:text=On%2011%20January%202019%2C%20Eurojust%2C%20in%20cooperation%20with,criminal%20use%20of%20encryption%20to%20hide%20illicit%20activities (consultado a 17/2/2023)

[90] EUROPOL/EUROJUST, "Common challenges in combating cybercrime", junho de 2019, p. 10, disponível em: https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf (consultado a 15/2/2023). No caso especificamente português, reporta-se o Relatório Anual de Segurança Interna de 2022, no que concerne a situações de exploração sexual de menores *online*, à «(…) produção, partilha e alojamento de conteúdos ilegais em plataformas encriptadas (…)» p. 66, disponível em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d (consultado a 5/6/2023).

[91] "First report of the observatory function on encryption" cit., p. 10. Tradução livre.

detiver tais chaves. Pode distinguir-se entre encriptação de dados em trânsito e encriptação de dados em repouso[92], sendo que a primeira visa a proteção da informação no processo de "viagem" entre o dispositivo de origem e o destinatário, protegendo-a de interferências externas não autorizadas[93]. Já a encriptação de dados em repouso visa salvaguardar a informação armazenada num determinado dispositivo ou servidor[94].

Em termos práticos, e perante a legislação atualmente em vigor, pensemos numa situação de acesso a um processo de comunicação por via de uma aplicação de mensagens instantâneas, como o *WhatsApp*. Estando em causa um fluxo de comunicação em tempo real, nomeadamente aplicações de mensagens, sendo hoje cada vez mais utilizada a chamada encriptação "ponta-a-ponta"[95] nas aplicações de comunicação, apenas o dispositivo emissor da mensagem e o recetor têm acesso às chaves[96], o que se traduz na impossibilidade de acesso ao conteúdo da mesma, independentemente dos servidores por onde passe a informação. Donde, perante uma comunicação encriptada, afigura-se inútil, por exemplo, a interceção de tal comunicação. Isto é, num contexto em que se pretenda ter acesso a um processo de comunicação, efetuado naquela aplicação, o método de investigação idóneo será a interceção de comunicações, prevista no artigo 18.º LCC[97], por regular o método de captação das comunicações entre o momento do envio e a chegada ao destinatário[98]. No entanto, estando esse fluxo protegido por encriptação "ponta-a-ponta", essa interceção seria tecnicamente impossível[99] (e, por isso, inútil), pois que mesmo que a comunicação atravesse um qualquer servidor, o mesmo não terá acesso ao seu conteúdo, uma vez que a chave de desencriptação da informação se encontra no dispositivo recetor. Por esta razão, apela-se à denominada "vigilância na fonte"[100] desse tipo de comunicações, captando a informação em forma desencriptada, o que será possível «infiltrando os computadores através de adequados programas do género "cavalo

[92] "First report of the observatory function on encryption" cit., p. 17
[93] *Ibidem*
[94] *Ibidem*
[95] *Ibidem*, p. 15; ARMANDO DIAS RAMOS, *O Agente Encoberto…,* cit., p. 123
[96] "First report of the observatory function on encryption" cit., p. 19
[97] No sentido da sua aplicação a aplicações de mensagens, PEDRO DIAS VENÂNCIO, *Lei do Cibercrime…,* cit., p. 119
[98] DAVID SILVA RAMALHO, *Métodos ocultos*…, cit., p. 339
[99] "Common challenges in combating cybercrime", cit., p. 10; ARMANDO DIAS RAMOS, *O Agente Encoberto…*, cit., p. 123
[100] MANUEL DA COSTA ANDRADE, "*Bruscamente no Verão Passado…"*, cit., pp. 164 e 165; BENJAMIM SILVA RODRIGUES, *Da Prova Penal*…, cit., p. 377

de Tróia"»[101], ou «lançando mão de específicos vírus informáticos de captação e intrusão»[102].

Por outro lado, as técnicas de encriptação são igualmente utilizadas em programas anonimizadores, que ocultam a origem do utilizador, garantindo-lhe anonimato na sua atuação, impedindo que se deixe uma "pegada digital" no acesso a qualquer *website*[103]. Um dos programas mais proeminentes é o *The Onion Router* (TOR), criado com o objetivo de impedir a interceção da comunicação e acesso ao conteúdo, bem como assegurando o anonimato do remetente, através de camadas de cifragem[104]. Também a utilização de *Virtual Private Networks* (VPN) se prende com objetivos de anonimização do utilizador, sendo a informação encriptada de modo a ocultar a ligação entre o dispositivo do utilizador e o servidor[105].

Ora, sendo a anonimização uma prioridade para os agentes do crime[106], e assistindo-se à "vulgarização" da criptografia com a proliferação dos *smartphones*[107], torna-se evidente como estas técnicas inutilizam os meios de investigação que as autoridades têm atualmente ao seu dispor. Nestas hipóteses, a única forma de se aceder aos dados será através da utilização de algum tipo de *malware.* Conforme referimos anteriormente, enviando um *software* para instalação no dispositivo do visado, permite-se ter acesso aos dados introduzidos pelo autor[108], ou, noutras palavras, acesso aos dados "na fonte" (trate-se ou não de uma comunicação)[109], contornando as barreiras impostas pelas técnicas de encriptação.

Sem pretensão de proceder a uma explicação exaustiva acerca de todo o tipo de técnicas de anonimização a que os agentes do crime recorrem, tentámos pôr a descoberto alguns dos desafios com que as autoridades de investigação se confrontam atualmente[110].

---

[101] MANUEL DA COSTA ANDRADE, "*Bruscamente no Verão Passado*…", cit., p. 165
[102] BENJAMIM SILVA RODRIGUES, *Da Prova Penal*…, cit., p. 378
[103] "First report of the observatory function on encryption" cit., p. 17
[104] DAVID SILVA RAMALHO, "A investigação criminal na Dark web", in *Revista de Concorrência e Regulação*, ano IV, nº14/15, abril-setembro, 2013, p. 390; "First report of the observatory function on encryption" cit., p. 17 «the software automatically creates a randomised path of different nodes, by 'borrowing' several other IP addresses for a session. Each node has its own layer of encryption, which includes information about the next connection. As a result, it becomes difficult to track the original IP address, as it is being disguised by three or more intermediate encrypted IP addresses».
[105] "First report of the observatory function on encryption" cit., pp. 18-19
[106] ARMANDO DIAS RAMOS, *O Agente Encoberto…,* cit., p. 134
[107] *Ibidem*, p. 155
[108] DAVID SILVA RAMALHO, "A investigação criminal na Dark web…", cit., p. 417
[109] ARMANDO DIAS RAMOS, *O Agente Encoberto…,* cit., p. 19
[110] Para uma explicação mais técnica e aprofundada acerca dos meios de anonimização utilizados pelos cibercriminosos, mas também sobre técnicas e soluções para os contornar, *vide* "First report of the

A resposta a estes obstáculos é, porém, complexa. Por um lado, a utilização de técnicas de *malware* no âmbito da investigação criminal exige, por parte dos OPC e MP, um conhecimento técnico elevado. Por outro, e indo mais de encontro ao que nos ocupa no presente trabalho, tratando-se de técnicas extremamente invasivas, que contendem com direitos fundamentais e colocam em causa princípios do processo penal, carecem de intervenção do legislador a quem incumbirá a ponderação entre os interesses de realização de justiça e de tutela dos direitos fundamentais.

Sendo esta uma temática que se encontra na ordem do dia, até ao nível das instâncias da UE[111], focar-nos-emos, em diante, na análise das técnicas de *malware* como método de obtenção de prova, no que diz respeito à sua natureza oculta e de compressão de direitos fundamentais e, posteriormente, na análise do tratamento dado a estas técnicas noutros ordenamentos jurídicos.

2.2. *MALWARE* COMO MÉTODO OCULTO DE OBTENÇÃO DE PROVA

Conforme ficou exposto supra, resulta da noção de *malware* que se trata de um *software* maligno instalado sub-repticiamente, estando a sua eficácia intimamente ligada ao seu caráter oculto. De facto, os novos desafios colocados à investigação em ambiente digital e os quais justificam, do ponto de vista da necessidade, o recurso ao *malware*, prendem-se com as possibilidades, por parte dos agentes do crime, de ocultarem os dados, e a sua identidade, por forma a despistar, dificultar e, até, impossibilitar, a investigação criminal. Ademais, a própria instalação do programa, como pudemos evidenciar em momento anterior, pressupõe que o visado não se aperceba de que está a ser alvo da diligência. Donde, e atenta a noção de métodos ocultos de prova, é evidente a inserção do *malware* nesta categoria de métodos de obtenção de prova.

Ora, no primeiro capítulo do presente trabalho abordámos a temática dos métodos ocultos de investigação em termos gerais, referindo que o potencial de devassa dos mesmos é substancialmente superior quando comparado com aquele dos métodos abertos, uma vez que, em virtude do seu caráter oculto, o grau de restrição dos direitos fundamentais é superior, além de serem colocados em risco direitos processuais que de outra forma (perante métodos abertos) estariam (mais) acautelados. Tendo já discorrido

observatory function on encryption" cit., e DAVID SILVA RAMALHO, "A investigação criminal na Dark web…", cit.

[111] Considerando n.º 27 da Diretiva 2011/92/EU do Parlamento Europeu e do Conselho; ARMANDO DIAS RAMOS, *O Agente Encoberto…,* cit., p. 157

acerca da problemática dos métodos ocultos de investigação, nomeadamente no que concerne à tensão constante entre a busca da verdade material e a proteção dos direitos fundamentais, cumpre agora analisar, em concreto, o grau de devassa comportado pela utilização de *malware,* e quais as consequências que tal tem (ou, pelo menos, deverá ter) a nível do regime legal deste específico método de obtenção de prova.

Através da explicitação dos vários modos de instalação de *malware* nos dispositivos, tivemos oportunidade de elencar algumas das inúmeras funcionalidades que este tipo de programas pode apresentar. Em bom rigor, a utilização de *malware* pode permitir às autoridades aceder a dados armazenados, não armazenados e produzidos em tempo real no sistema instalado[112], bem como ligar o microfone e a câmara do dispositivo visado (ativação do *hardware*), e registar as teclas por ele premidas[113]. No fundo, a utilização de *malware* permite monitorizar toda a atividade desenvolvida no seio de um determinado sistema informático, o que se traduz na possibilidade de, em bom rigor, *espiar* um determinado sistema, com acesso ilimitado a toda a informação[114] aí presente, o que lhe confere uma qualificada danosidade social, tornando-o um método *mais gravoso* em comparação com outros[115], mesmo dentro da categoria de métodos ocultos.

Não existindo uma hierarquia legalmente definida dos vários métodos ocultos[116], é possível, contudo, estabelecer uma hierarquização em função do grau de lesão de direitos fundamentais comportado. Nomeadamente, COSTA ANDRADE[117] avança um exemplo relativamente à maior danosidade social das gravações de conversas entre presentes, em relação às escutas telefónicas, de tal modo que, numa tentativa de hierarquização dos métodos ocultos existentes, sempre terá de se reconhecer a acrescida danosidade daquelas em relação a estas. Da mesma forma, atento o elevado potencial lesivo do *malware*, que restringe em enorme grau um vasto leque de direitos fundamentais, poderá este merecer o título de «meio de obtenção da prova mais invasivo e intensamente restritivo de direitos fundamentais»[118], o que implica um cuidado acrescido na sua utilização e consagração do respetivo regime.

---

[112] JULIANA SOUSA CAMPOS, *O Malware…,* cit. p. 57
[113] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 324
[114] É de realçar, neste âmbito, também a *quantidade* e *qualidade* da informação a que é possível aceder num sistema informático.
[115] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 354
[116] JULIANA SOUSA CAMPOS, *O Malware…,* cit. p. 56
[117] MANUEL DA COSTA ANDRADE, "Métodos ocultos de investigação…", cit., p. 538
[118] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 351

Entendemos, assim, que o debate acerca da admissibilidade de utilização de *malware* no âmbito da investigação criminal depende de uma análise sobre o seu grau de invasividade nos direitos fundamentais por, essencialmente, duas ordens de razão: 1) para delimitação da sua consagração legal, uma vez que as potencialidades técnicas deste método têm, necessariamente, de ser limitadas, num primeiro momento, através do regime legal, e num segundo momento, através da delimitação dos dados a recolher na autorização judicial[119]; 2) para se dar cumprimento ao princípio da subsidiariedade[120].

Desde logo, evidentemente que, por forma a dar cumprimento às exigências do artigo 18.º, nº2 CRP, aquando da consagração de um método de obtenção de prova, tem de se proceder a uma análise dos direitos fundamentais atingidos, bem como ao modo e grau dessa lesão. No que concerne especificamente à utilização de *malware,* vimos que este método pode revestir inúmeras funcionalidades, o que se repercute necessariamente ao nível da intromissão nos direitos fundamentais do visado. Assim, não só tem este meio aptidão para restringir diversos direitos fundamentais, como essa lesão pode comportar graus variados. É então da maior importância proceder a uma análise cuidada dos direitos em causa e do respetivo grau de compressão, pois tal levar-nos-á a concluir que nem todas as funcionalidades permitidas pelo *malware* serão legítimas nas mesmas circunstâncias, à luz da CRP, pelo que entendemos que não se deve procurar um regime legal unitário aplicável ao *malware*, sob pena de se permitir uma monitorização do visado desproporcional em face aos fins da investigação[121].

Por outro lado, o recurso a meios ocultos de obtenção de prova deve fazer-se no estrito cumprimento do princípio de subsidiariedade, em termos de que a opção por qualquer método de obtenção de prova deve fazer-se desde que não exista um outro método menos lesivo suscetível de alcançar os mesmos resultados de investigação[122], já que, de outra forma, não estará legitimada a violação dos direitos fundamentais decorrente da utilização de um determinado método de prova. Aquando da consagração legal de qualquer método de obtenção de prova, incumbe ao legislador dar cumprimento ao princípio da proporcionalidade nos termos do artigo 18.º, nº2 CRP, estando ínsita na norma legal habilitadora a *necessidade*, em abstrato, de consagração daquele método de

[119] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 349
[120] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…"* cit., pp. 114 e 115
[121] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 349
[122] Efetivamente, tal requisito encontra-se expresso na regulação do regime das escutas telefónicas, nos termos do artigo 187.º, nº1 CPP

prova. Não obstante, *in casu*, cumprirá à autoridade judiciária (em princípio, no seio de métodos ocultos, o JIC) ponderar, com base no regime legal consagrado, a (in)existência de meios menos lesivos que permitam alcançar os mesmos resultados, à luz do princípio da subsidiariedade. Para se fazer este juízo é, portanto, necessário compreender o grau de lesão e devassa comportado por cada método de prova.

Ao analisar os direitos comprimidos pelo recurso a técnicas de *malware*, cumpre desde logo mencionar a decisão do BVerfG de 27 de fevereiro de 2008[123], a qual versou, essencialmente, sobre a admissibilidade da infiltração oculta em sistemas tecnológicos, em termos semelhantes àqueles em que opera o *malware*[124], o que explica a pertinência da referência desta decisão para o presente trabalho. Tendo analisado a problemática à luz dos direitos fundamentais à privacidade das telecomunicações[125], à inviolabilidade do domicílio[126], e à autodeterminação informacional[127], o tribunal concluiu que o concreto método de obtenção de prova em causa, não contendendo sempre necessariamente com o âmbito de proteção dos restantes direitos mencionados, contendia, sim, com o direito à integridade e confidencialidade dos sistemas informáticos[128], enquanto manifestação do direito geral de personalidade.

Efetivamente, perante as novas ameaças para a personalidade decorrentes do progresso tecnológico, assiste-se à expansão do âmbito de proteção dos direitos fundamentais já reconhecidos, ou à emergência de novos direitos, em virtude do «desvelamento e reconhecimento de novas dimensões da personalidade»[129]. Donde, percebe-se que o BVerfG, reconhecendo que uma área da personalidade carecida de proteção constitucional não a encontraria no âmbito de outros direitos já reconhecidos e consolidados, tenha decantando este novo direito. O direito fundamental à integridade e confidencialidade dos sistemas informáticos «atualiza a proteção da personalidade à

---

[123] Decisão proferida no âmbito da fiscalização da conformidade constitucional do §5(2) n.º11 a Lei de Proteção da Constituição da Renânia do Norte-Vestefália

[124] BVerfG, Decisão do Primeiro Senado, de 27 de fevereiro de 2008 - 1 BvR 370/07 -, parágrafo 5, disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html . Realçando expressamente as semelhanças do programa utilizado pela lei sob fiscalização em relação ao malware, como os Cavalos de Tróia e os vírus, veja-se WIEBKE ABEL/BURKHARD SCHAFER, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822" *SCRIPTed – A Journal of Law, Technology and Society*, Volume 6, n.º 1, April 2008, p.109, disponível em http://script-ed.org (consultado a 21/3/2023)

[125] BVerfG - 1 BvR 370/07 - parágrafo 183 e ss.

[126] *Ibidem*, parágrafo 191 e ss.

[127] *Ibidem*, parágrafo 198 e ss.

[128] *Ibidem*, parágrafo 201

[129] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…"*, cit., p. 113

realidade tecnológica do século XXI.»[130]. Não obstante, a proclamação da existência deste direito no nosso ordenamento jurídico não atingiu ainda, em nosso entender, o desejado patamar de solidez e consistência. Isto é, encontramos apenas escassas referências a este direito na doutrina[131], e na jurisprudência[132] reconhece-se a integridade e confidencialidade dos sistemas informáticos enquanto bem jurídico protegido nos crimes de falsidade informática e de acesso ilegítimo (p. e p., respetivamente, nos artigos 3.º e 6.º LCC).

Indo buscar inspiração à mencionada decisão do BVerG, mas fazendo a análise dos direitos fundamentais colocados em causa pela utilização de *malware* à luz do nosso paradigma constitucional, analisaremos individualmente os direitos já referidos, mas abordaremos igualmente a problemática da existência de uma área nuclear inviolável da privacidade, uma vez que os restantes direitos mais não são do que manifestações concretas da tutela amplamente concedida à privacidade.

2.2.1. DIREITO À INVIOLABILIDADE DOMICÍLIO: EM QUE TERMOS PODE SER COMPRIMIDO PELA UTILIZAÇÃO DE TÉCNICAS DE *MALWARE*

O direito à inviolabilidade do domicílio encontra-se consagrado no artigo 34.º CRP, estando a admissibilidade da sua restrição para efeitos da lei penal desde logo expressa, e delimitada, nos nºs 2 e 3 do mesmo artigo. No entanto, pode ser uma tarefa árdua definir aquilo que se entende por «domicílio», e por violação do mesmo, especialmente ao falarmos de sistemas informáticos, dado que se trata de uma realidade digital, por oposição a uma realidade física onde se afigura menos complexo delimitar um domicílio, enquanto local onde se habita[133]. Em nosso entender, podemos abordar a problemática da inviolabilidade do domicílio, neste contexto, de duas perspetivas: 1)

---

[130] RAINER ERD, *apud* FABIANO MENKE, "A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão", in *Revista Jurídica Luso-Brasileira*, Ano 5, nº 1, 2019, p. 795

[131] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…",* cit., p. 113; RITA CASTANHEIRA NEVES, *As ingerências nas comunicações eletrónicas em processo penal,* Coimbra, Coimbra Editora, 2011, p. 147; JULIANA SOUSA CAMPOS, *O Malware…*, cit., p. 57; , JOÃO GOUVEIA CAIRES, "Métodos ocultos na criminalidade económico-financeira…", cit., p. 80. BENJAMIM SILVA RODRIGUES aprofunda mais esta problemática, questionando a necessidade de decantação deste direito, em virtude do seu âmbito de proteção poder ser acautelado por outros direitos existentes, cfr. BENJAMIM SILVA RODRIGUES, *Da Prova Penal…,* cit., p. 474

[132] Ac. TRE, proc. 82/20.9PACTX-A.E1, de 25-05-2021, Rel. Martinho Cardoso; Ac. TRG, proc. 19/19.8GCBRG.G1, de 12-04-2021, Rel. Paulo Serafim; Ac. TRP, proc. 1001/11.9JAPRT.P1, de 21-11-2012, Rel. Borges Martins; Ac. TRL, proc. 368/16.7JAPDL.L1-3, de 09-01-2019, Rel. Nuno Coelho. Esta orientação não é, contudo, consensual, havendo quem discorde de que o bem jurídico protegido é a integridade e confidencialidade dos sistemas informáticos.

[133] J.J. GOMES CANOTILHO / VITAL MOREIRA, *Constituição da República…,* cit., p. 540

adotando um conceito de «domicílio informático-digital»[134], o qual seria violado pela utilização de *malware*; 2) rejeitando a ideia de «domicílio informático-digital» enquanto domicílio para efeitos da proteção do artigo 34.º CRP, mas reconhecendo que, hoje em dia, a violação e devassa do domicílio podem ser efetuadas por via de meios eletrónicos[135], não dependendo da entrada física na morada de alguém.

A primeira das perspetivas é avançada e defendida por BENJAMIM SILVA RODRIGUES[136], segundo uma ideia de que o computador (e, bem assim, outros dispositivos, como *smartphones* ou *tablets*) é, hoje, «a "casa digital" onde mora a nossa "alma digital" (…) e entrar [nele] é colocar um pé em casa do seu titular (…)»[137]. Ora, reconhecendo o mérito devido àquilo a que o autor se refere, no sentido de que, nos dias que correm, o dispositivo pessoal de alguém configura, verdadeiramente, uma das facetas mais íntimas da sua vida, entendemos que não aproveita da proteção conferida ao domicílio pelo artigo 34.º CRP. Efetivamente, a vida privada desenrola-se nos telemóveis e computadores dos cidadãos, e, assim, a tutela conferida à privacidade e intimidade de cada pessoa através da inviolabilidade do domicílio deve igualmente ser conferida aos dispositivos informáticos, pois que a privacidade que se pretende acautelar com a proteção da inviolabilidade do domicílio, e colocada em crise pela sua devassa, sê-lo-á igualmente por vias de intromissão nos dispositivos informáticos de cada um. Não obstante, e sendo o domicílio e os sistemas informáticos "espaços" da intimidade de cada um, não deixam de configurar realidades substancialmente diferentes, não sendo possível, em nosso entender, transpor a proteção conferida ao domicílio pelo artigo 34.º CRP para os sistemas informáticos. O que reclama a tutela nos termos do artigo 34.º CRP é o comportamento e desenvolvimento da vida privada que, primordialmente, acontece dentro do domicílio[138], mas nem por isso se justifica que qualquer local onde se desenrolem aspetos da vida íntima mereça a caracterização de domicílio. Sendo a proteção constitucional conferida ao domicílio uma manifestação concreta da proteção da

[134] BENJAMIM SILVA RODRIGUES, *Da Prova Penal…,* cit., p. 473
[135] J.J. GOMES CANOTILHO / VITAL MOREIRA, *Constituição da República…,* cit., p. 541
[136] BENJAMIM SILVA RODRIGUES, *Da Prova Penal…,* cit., p. 473
[137] *Ibidem*
[138] MANUEL DA COSTA ANDRADE, "Domicílio, Intimidade e Constituição (anotação crítica do acórdão 364/2006 do Tribunal Constitucional)" in *Revista Brasileira de Ciências Criminais*, ano 21, vol. 100, janeiro-fevereiro de 2013, p. 62

vida privada, domicílio e privacidade/intimidade não se confundem nem se representam e implicam reciprocamente[139].

No que concerne à segunda perspetiva mencionada, a problemática prende-se com o *modo* de violação do domicílio, e já não com aquilo que se pode entender por domicílio para efeitos do artigo 34.º CRP. Ora, atualmente, é tecnicamente possível a intromissão no domicílio de outrem que não passe pela presença física. Tem-se entendido[140] que cabem no âmbito de proteção da norma situações de devassa «concretizadas já através da introdução e presença no domicílio de meios técnicos de escuta, de transmissão de imagens ou de sons (…)»[141], sendo que o que confere merecimento de tutela do domicílio é a circunstância de a intromissão operar sobre o «espaço fisicamente delimitado da habitação (…) mesmo que sem a entrada (e presença) física do agente»[142]. Ora, uma das funcionalidades do *malware* prende-se precisamente com a possibilidade de ativar o microfone e a câmara do dipositivo do visado, pelo que, quando este se encontre na habitação, então haverá violação do domicílio, nos termos expostos.

Contudo, entendemos que a compressão deste direito pela utilização de técnicas de *malware* será rara, porque depende de o dispositivo atacado se encontrar dentro de um domicílio *e* da concreta funcionalidade do *malware* utilizada. Isto é, desde logo, apenas poderíamos estar sob o âmbito de proteção do artigo 34.º, nº2 CRP nos casos em que o dispositivo se encontrasse, efetivamente, no domicílio. Ora, sendo que a infiltração no sistema, através de *malware*, pode ocorrer independentemente do local físico onde se encontre o mesmo, inúmeros casos não seriam abrangidos pela tutela conferida ao domicílio. Além disso, o local físico onde se encontra o sistema informático visado pela diligência é, as mais das vezes, irrelevante no sentido de que aquilo a que se pretende aceder é ao conteúdo do sistema. Ademais, mesmo que o dispositivo se encontre dentro do domicílio, se a utilização de *malware* se consignar ao acesso ao conteúdo do sistema informático, sem ativação do *hardware* do dispositivo, nunca haverá afetação do direito à inviolabilidade do domicílio. Como referimos supra, cremos que poderá haver agressão a este direito quando se aceda à câmara e ao microfone, havendo, desse modo, a «ultrapassagem de uma barreira (…) tecnológica»[143].

---

[139] MANUEL DA COSTA ANDRADE, "Domicílio, Intimidade e Constituição…", cit., p. 75
[140] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…",* cit., p. 152
[141] *Ibidem*
[142] *Ibidem*
[143] MANUEL DA COSTA ANDRADE, "Domicílio, Intimidade e Constituição…", cit., p. 65

Aqui chegados, suscita-se outra relevante questão: até que ponto é legítima a utilização de *malware* para ativação da câmara e microfone do dispositivo? Sendo-o, deverá permitir-se esse grau de «espionagem» dentro do domicílio?

Desde logo, cumpre ter presente que o artigo 6.º da Lei n.º5/2002, que regula as medidas de combate à criminalidade organizada, permite o registo de voz e imagem, por qualquer meio, mesmo sem o consentimento do visado. Ora, não pretendendo discutir qual a amplitude de «qualquer meio», entendemos que, a proceder à consagração expressa da utilização de técnicas de *malware*, não será de excluir liminarmente a possibilidade de recurso às mesmas para recolha de prova externa, ativando a câmara e o microfone do dispositivo. Mais problemática se afigura a questão de saber se por essa via se permite o registo de voz e imagem no âmbito do domicílio[144], sob pena de se permitir uma desproporcionada monitorização do visado. Conforme veremos no capítulo 2.3. do presente texto, na StPO encontra-se prevista a possibilidade de recurso a técnicas de *malware* para interceção de conversas entre presentes, em locais privados, estando a sua utilização, contudo, sujeita a apertados requisitos e garantias de modo a proteger a área inviolável da vida privada. Não obstante, é imperativo reconhecer que as circunstâncias em que é atingido o direito à inviolabilidade do domicílio através da utilização de *malware* são extremamente invasivas e aproximar-se-ão daquilo que a doutrina apelida de *Lauschangriff*[145].

Donde, o direito à inviolabilidade do domicílio é suscetível de ser afetado pela utilização de *malware*, mas sê-lo-á de forma residual, e não deve ser, em nosso entender, o ponto central de análise, pois é insuficiente para conferir proteção a todos os riscos e ameaças decorrentes deste tipo de agressão, não protegendo sequer contra os mais comuns.

2.2.2. O RECURSO A TÉCNICAS DE *MALWARE* E O SIGILO DAS TELECOMUNICAÇÕES

Do ponto de vista do sigilo das telecomunicações, teremos de delimitar a nossa análise.

[144] CARLOS RODRIGUES DE ALMEIDA, "O registo de voz e imagem – notas ao artigo 6.º da lei nº5/2002, de 11 de janeiro", in *Revista Portuguesa de Ciência Criminal*, ano 14, nº3, julho-setembro 2004, p. 376
[145] MANUEL DA COSTA ANDRADE, "*Bruscamente no Verão Passado…",* cit., p. 111

Desde logo, defende-se que no âmbito das buscas *online*[146], não há, em bom rigor, intromissão nas telecomunicações[147], porque, embora se recorrendo à *internet*, nem tudo o que implica um sistema de telecomunicação é em si uma telecomunicação[148]. Muito embora assim o seja, a verdade é que, não comportando toda a infiltração num sistema informático por via de *malware* uma intromissão nas telecomunicações, ela *pode* efetivamente consubstanciar uma intromissão nas telecomunicações, sendo um entendimento daquele tipo um tanto redutor da complexidade da figura do *malware*. Em bom rigor, por via da utilização de *malware* é tecnicamente possível a interceção de comunicações, o que contende, evidentemente, com o direito à inviolabilidade das telecomunicações, previsto no artigo 34.º, nº4 CRP. Porém, a "mera" interceção de comunicações encontra-se prevista nos artigos 18.º LCC e 187.º e ss. CPP, pelo que, em função do princípio da subsidiariedade, não se deverá recorrer à utilização de *malware* para esse efeito, sob pena de, ao "infetar" o sistema do visado, se colocar em crise outros direitos. Esta é, em nosso entender, a primeira questão a colocar no âmbito da análise da violação da privacidade das comunicações através da utilização de *malware*.

Não obstante, como explicitámos anteriormente, o recurso ao *malware* permite que as autoridades procedam à vigilância na fonte de determinadas comunicações, de modo a ter acesso ao seu conteúdo antes de este ser encriptado, ou após a sua desencriptação, residindo neste aspeto uma das grandes valias da utilização de *malware* na investigação criminal. Perante isto, levantam-se problemas acerca da sua inserção, ou não, no âmbito de tutela da inviolabilidade das telecomunicações, nos termos do artigo 34.º, nº4 CRP. O ponto da questão reside no facto de, com a vigilância na fonte, ainda não se ter dado início ao processo dinâmico de transmissão, ou então já o mesmo ter terminado[149], levando-nos a questionar se esse ato caberá, então, no fundamento da tutela à inviolabilidade das telecomunicações. Em bom rigor, a «tutela jurídica da inviolabilidade das telecomunicações radica na "específica situação de perigo" decorrente do domínio que o terceiro detém – e enquanto o detém – sobre a comunicação»[150] estando a tutela da inviolabilidade das telecomunicações «vinculada ao processamento da

[146] Estamos a referir-nos a buscas online na medida em que a doutrina se refere às mesmas, não utilizando o conceito de *malware*, mas referindo-se à mesma realidade
[147] BENJAMIM SILVA RODRIGUES, *Da Prova Penal…,* cit., p. 474
[148] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…",* cit., p. 156
[149] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 340
[150] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…",* cit., p. 158

comunicação sob o domínio da empresa fornecedora do serviço de telecomunicações»[151]. Porém, também não se dirá que estamos, em bom rigor, perante mensagens que possam configurar dados armazenados. Já a propósito do correio eletrónico foi intensamente debatida na doutrina e na jurisprudência tutela conferida aos *e-mails* abertos armazenados, no sentido de saber se um *e-mail* aberto e marcado como lido, carece ainda de tutela do sigilo das telecomunicações, ou se configura já um mero dado informático, caindo fora desse âmbito de tutela. A querela resulta da orientação tradicional de distinção entre apreensão de correspondência aberta e fechada, no âmbito do CPP, e mesmo perante a letra do artigo 17.º LCC encontra-se na doutrina[152] quem defenda a diferenciação de regime aplicável consoante a mensagem de correio eletrónico tenha sido ou não lida. Esta orientação baseia-se no pressuposto de que, uma vez chegada ao destinatário e aberta a mensagem, cessa o processo comunicacional[153], e, por isso, cessa também a tutela constitucional da inviolabilidade das telecomunicações. Por outro lado, e reconhecendo a dificuldade inerente em estabelecer a fronteira entre o correio eletrónico lido ou não lido[154], muita doutrina[155] defende que, nos termos do artigo 17.º LCC não há lugar a tal distinção, sendo toda a apreensão de correio eletrónico ordenada pelo JIC. Não obstante, não colocam em causa que tenha terminado o processo comunicacional. Por via desta argumentação, poderíamos ser levados a crer que, nos casos de vigilância na fonte, em que a mensagem não se encontra em trânsito, também não estaria em causa a tutela constitucional das telecomunicações.

Não obstante, parece-nos indiscutível que, em tais casos, nos encontramos ainda no âmbito do processo comunicacional, carecido da tutela conferida pelo artigo 34.º, nº4 CRP. É entendimento do TC que o direito à autodeterminação comunicativa se configura

---

[151] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…",* cit., p. p. 159

[152] JOÃO CONDE CORREIA, "Prova Digital…", cit., p. 41; PAULO DÁ MESQUITA, *Processo Penal…,* cit., p. 118; DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova previstos na lei do cibercrime*, 1ª ed., Coimbra, Gestlegal, 2018, p. 145

[153] Neste sentido, MANUEL DA COSTA ANDRADE, "*Bruscamente no Verão Passado*…", cit., p. 159 «(…) depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito».

[154] Efetivamente, para marcar como lida uma mensagem de correio eletrónico ou outra mensagem de natureza semelhante, basta um clique, o qual é reversível. Ademais, a mesma mensagem pode encontrar-se em vários dispositivos, aparecendo nuns e noutros como lida ou não lida.

[155] DAVID SILVA RAMALHO, *Métodos Ocultos…,* cit., p. 278 e 279; SÓNIA FIDALGO, "A Recolha De Prova Em Suporte Electrónico — Em Particular, A Apreensão De Correio Electrónico", in *Julgar*, nº 38, 2019, p. 159 e 160; RUI CARDOSO, "Apreensão de Correio Eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei 109/2009, de 15.IX", in *Cibercriminalidade e Prova Digital*, Coleção Formação Contínua, CEJ, 2018, p. 71; RITA CASTANHEIRA NEVES, *As ingerências nas comunicações…,* cit., p. 276. Esta autora refere um "plus" de proteção conferido pelo legislador aos e-mails armazenados, em nome da autodeterminação informacional.

como «um direito de liberdade, de liberdade para comunicar, sem receio ou constrangimentos de que a comunicação ou as circunstâncias em que a mesma é realizada possam ser investigadas ou divulgadas»[156], estando, por isso, necessariamente, os momentos imediatamente anterior e posterior ao processo dinâmico de transmissão da comunicação compreendidos nessa liberdade, e assim tutelados no âmbito do direito à inviolabilidade das telecomunicações. No recente ac. nº 91/2023[157], o TC reitera o entendimento segundo o qual o fundamento subjacente à cessação da tutela constitucional das comunicações tem que ver com a possibilidade de o destinatário, uma vez lida a mensagem, poder adotar e desenvolver a proteção que entender. Ora, evidentemente que tal possibilidade não está em causa quando se opere a vigilância na fonte – seja porque a comunicação foi acedida previamente ao momento de encriptação, seja porque foi acedida em simultâneo com o destinatário, aquando da desencriptação. Por outro lado, a maioria dos argumentos no sentido de que não se está perante um processo comunicativo no que concerne aos *e-mails* já abertos prendem-se com o facto de a mensagem se encontrar na posse do destinatário, o que naturalmente é intransponível para o caso da vigilância na fonte da comunicação no terminal do remetente. Assim, salvo melhor opinião, entendemos que dificilmente se pode argumentar que o recurso ao *malware* não comprime o direito ao sigilo das telecomunicações, uma vez que tal significaria deixar excluídas do seu âmbito de proteção realidades que reclamam essa tutela. Ademais, o facto de as situações de vigilância na fonte das comunicações encontrarem a sua legitimação no facto de não ser possível a tradicional interceção da comunicação em trânsito, por a mesma se encontrar encriptada, leva-nos a crer que o direito em causa é o mesmo, diferindo no caso o modo ou o momento da agressão.

Posto isto, entendemos que a utilização de *malware* tem potencial de devassa das telecomunicações, convocando a tutela constitucional das mesmas. No entanto, tal como refere DAVID SILVA RAMALHO[158], este método de investigação não se encontra abrangido nem tão-pouco legitimado pelas normas que tradicionalmente se referem à intromissão nas telecomunicações. Tal não advém, contudo, de não estar em causa uma possível intromissão no processo comunicativo[159], mas antes do facto de tais normas processuais

[156] Ac. TC nº268/2022, proc. nº828/2019, Rel. Conselheiro Afonso Patrão
[157] Ac. TC nº91/2023, proc. nº559/2020, Rel. Conselheira Joana Fernandes Costa
[158] DAVID SILVA RAMALHO, *Métodos Ocultos*…, cit., p. 341
[159] Neste sentido, veja-se igualmente MANUEL DA COSTA ANDRADE, "*Bruscamente no Verão Passado…",* cit., p. 165, na medida em que embora não se encontrado legitimada pelas normas que legitimam a interceção nas comunicações, viola-se esse direito. Também, BENJAMIM SILVA RODRIGUES, *Da Prova*

não preverem expressamente a utilização de um específico *software* para interceção e gravação das comunicações na fonte, para se ter acesso às mesmas na forma desencriptada, à semelhança daquilo que se verifica no ordenamento jurídico alemão, como veremos infra.

Não querendo precipitar-nos no avanço de certas conclusões, que aprofundaremos adiante, cremos que o entendimento de que não está em causa a intromissão nas telecomunicações advém de uma abordagem à temática da utilização de *malware* no âmbito da investigação criminal, em nosso entender, errada, por não tomar em consideração que, dada a complexidade técnica e as imensuráveis possibilidades de programação de um *software*, os modos de invasão e agressão dos direitos não merecem todos o mesmo tratamento. Em bom rigor, não está em causa a utilização de *malware,* como um todo em si com características definidas e estanques, mas antes a utilização de técnicas de *malware.*

O direito à inviolabilidade das telecomunicações poderá indubitavelmente ser comprimido através da utilização de *malware*, sendo essencial, para que tal seja legítimo, a consagração da admissibilidade legal deste tipo de intromissão em telecomunicações, sendo preferível uma regulação que acautele que o *software* utilizado se cinge à intromissão na esfera do visado na medida do estritamente necessário, impedindo-se o recurso a outras funcionalidades que extravasem o acesso às comunicações na fonte.

2.2.3. A UTILIZAÇÃO DE *MALWARE* E A AFETAÇÃO DOS DIREITOS À AUTODETERMINAÇÃO INFORMATIVA E À INTEGRIDADE E CONFIDENCIALIDADE DOS SISTEMAS INFORMÁTICOS

Na medida em que através da infiltração oculta num sistema informático por via da instalação de *malware* no mesmo se pode aceder aos dados pessoais do visado, também se estará perante a violação do direito fundamental à autodeterminação informativa, previsto no artigo 35.º CRP. Este direito compreende um conjunto de direitos que tutelam cada cidadão perante a recolha, processamento e tratamento automático de dados pessoais, bem como perante «outras utilizações possibilitadas pelas novas tecnologias»[160], sendo que a sua consagração confere ao titular o poder de decidir sobre

Penal…, cit., p. 379 «(…) havendo (…) a confluência da lesão, com um único ato, simultaneamente de dois direitos fundamentais e apenas estando prevista a admissibilidade da lesão de um deles».

[160] CATARINA SARMENTO E CASTRO, "40 Anos de «Utilização da Informática» — O artigo 35.º da Constituição da República Portuguesa", in *e-Pública*, vol. 3, n.º 3, 2016, p. 44

o uso e divulgação dos seus dados[161]. Embora nem sempre este direito seja violado, e desse modo a tutela por si conferida não baste para referenciar todos os casos de recurso ao *malware*, terá necessariamente de se ter em conta, na consagração deste regime legal, os limites impostos pelo direito à autodeterminação informativa[162].

Por sua vez, é também indubitavelmente comprimido o direito à confidencialidade e integridade dos sistemas informáticos. Ao contrário daqueles referidos anteriormente, entendemos que este direito será sempre comprimido, independentemente da funcionalidade concreta do *malware* utilizada. Em bom rigor, a utilização deste método de investigação consistirá sempre na infiltração oculta num sistema informático, para posteriormente se proceder à sua execução. Com efeito, nos termos expostos pelo BVerfG, este direito tutela os sistemas informáticos, como um todo, contra ingerências ocultas[163]. Os sistemas informáticos contêm consabidamente uma quantidade quase imensurável de dados de diferentes qualidades, de tal forma que o acesso a tais sistemas coloca, por si só, à descoberta aspetos da vida privada, e não só, do utilizador[164]. No âmbito deste direito, o seu titular encontra tutela relativamente ao acesso oculto ao sistema informático através do qual toda a informação aí contida seja suscetível de ser acedida em larga escala[165].

Todos os direitos anteriormente referidos encontram a sua tutela dependente da intromissão concreta no seu âmbito de tutela, ou seja, dependente da intromissão no domicílio, nas telecomunicações, ou do acesso ou tratamento de dados pessoais. Não obstante, a mera instalação sub-reptícia de um programa num determinado sistema informático contende com a integridade e confidencialidade desse sistema, a qual deve ser tutelada e por essa razão que o BVerfG tenha decantando este novo direito fundamental, de molde a não deixar desprotegida esta área.

[161] Ac. TC nº268/2022, cit.
[162] Nomeadamente, «é imperioso que os cidadãos conheçam que os seus dados foram acedidos; que possam eficazmente controlar o modo como são alcançados, controlados e tratados; e que possam recorrer aos tribunais para reagir contra a sua utilização indevida», para o que o visado deve ser informado acerca dos meios ocultos de investigação de que tenha sido alvo, quando tal notificação não ponha em causa o sucesso da investigação. Cfr. Ac. TC nº268/2022, cit.
[163] BVerfG - 1 BvR 370/07 - parágrafo 203
[164] BVerfG - 1 BvR 370/07 - parágrafo 203
[165] BVerfG - 1 BvR 370/07 - parágrafo 205

2.2.4. DIREITOS AFETADOS COMO MANIFESTAÇÕES DO DIREITO À RESERVA DA VIDA PRIVADA

Todos os direitos acabados de analisar, tendo âmbitos de proteção distintos e autónomos, podem ser modelados como direitos-garantia do direito à reserva da intimidade da vida privada[166], consagrado no artigo 26.º, nº1 da CRP e objeto de uma garantia no n.º2 do mesmo artigo.

Como vimos, a restrição de todos aqueles direitos é legítima mediante observação de determinados requisitos e condições, sendo um deles, necessariamente, o respeito pelo núcleo irredutível da vida privada. Conforme mencionámos anteriormente, o direito processual penal, em especial em matéria de prova, carece de encontrar um equilíbrio ótimo entre a descoberta da verdade material e o respeito pelos direitos fundamentais, sendo que, mediante as circunstâncias, prevalecerá um ou outro. À semelhança do que vale para os direitos anteriormente analisados, o próprio direito "geral" à privacidade não pode configurar-se, em geral, como absoluto e ilimitável[167], o que é de resto evidenciado pela admissibilidade de restrições à vida privada no âmbito do processo penal, nos termos do artigo 34.º CRP e 126.º, n.º3 CPP, e as quais temos vindo a analisar. Não obstante, importa reconhecer uma área da vida privada reportada «ao domínio nuclear intocável da personalidade e, inerentemente, a dignidade do homem»[168], a qual deve ser acautelada e se encontra subtraída a um juízo de ponderação, ainda que isso implique um sacrifício dos interesses gerais da investigação e da prossecução da justiça penal[169].

O debate acerca da admissibilidade de valoração de conteúdos de diários íntimos, iniciado na jurisprudência alemã[170], permitiu à doutrina e jurisprudência nacionais desenvolver a problemática do confronto entre a intimidade e o direito à vida privada e a eficácia do sistema penal, sendo atualmente consensual que «o direito à reserva da intimidade da vida privada não deixa de redundar na tutela jusfundamental de uma "esfera pessoal íntima" (…) e "inviolável" (…) de "um núcleo mínimo onde ninguém penetre salvo autorização do próprio titular" (…)»[171] e que «não [se] pode dispensar, (…) a

[166] Ac. TC nº268/2022, cit.
[167] Ac. TC nº607/2003, proc. nº 594/03, Rel. Benjamim Rodrigues
[168] TC nº607/2003, cit.
[169] MARIA FERNANDA PALMA, "Tutela da vida privada e Processo Penal (soluções para o conflito de valores na jurisprudência constitucional)", in *Estudos em memória do Conselheiro Luís Nunes de Almeida*, Coimbra, Coimbra Editora, 2007, p. 663
[170] MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova em processo penal*, 2ª ed., Coimbra, Gestlegal, 2022, p. 31
[171] Ac. TC nº607/2003, cit.

consideração do limite, ineliminável e intransponível, da dignidade e da integridade da pessoa humana.»[172].

No que ao nosso tema diz respeito, tendo em conta a quantidade e natureza de dados a que é possível aceder no seio de um sistema informático, tem de se acautelar que não são acedidos, e muito menos recolhidos, dados atinentes à área nuclear da vida privada, mesmo quando estejam em causa as formas mais drásticas de criminalidade[173]. Donde, permitindo-se a utilização deste método de obtenção de prova, o qual comporta a devassa da vida privada, de diversos modos, terá sempre de se acautelar o respeito por esta área inviolável da vida privada[174], sem prejuízo de uma tal violação comportar sempre uma proibição de valoração da prova independente[175].

2.2.5. GARANTIAS PROCESSUAIS E AFETAÇÃO DE TERCEIROS

Não olvidamos que o recurso a este tipo de técnicas, configurando um método oculto de obtenção de prova, viola determinados princípios processuais e direitos de defesa do arguido, nomeadamente, o privilégio contra a autoincriminação e o direito ao silêncio[176]. Porém, não é novidade que a lei admite o recurso a métodos ocultos (p.e., escutas telefónicas, ações encobertas, escutas ambientais) que, por si, "impedem" que o arguido exerça aqueles direitos. A lei fá-lo após a ponderação dos interesses em jogo, nomeadamente o interesse público na realização da justiça, propendendo para, em determinados casos e mediante a verificação de determinados requisitos, autorizar este tipo de métodos. Sob pena de inconstitucionalidade, a lei rodeia, por exemplo, o regime das escutas telefónicas de determinados condicionamentos restritivos que as tornem admissíveis no nosso paradigma constitucional e processual penal, mesmo suprimindo garantias processuais do arguido, nos termos do artigo 32.º, nº1 CRP. Em nosso ver, a utilização de *malware* na investigação criminal, suscitando igualmente questões controversas no que concerne às garantias processuais do arguido e até numa lógica de

[172] Ac. TC nº607/2003, cit.
[173] MANUEL DA COSTA ANDRADE, "Domicílio, Intimidade e Constituição…", cit., p. 84
[174] Tal é possível, por exemplo, à luz do parágrafo §100d do StPO, que determina a inadmissibilidade das medidas de interceção de comunicações (telefónicas ou entre presentes) e buscas *online* quando tal resulte na violação da área nuclear da vida privada.
[175] Isto é, mesmo que não existisse uma proibição de produção da prova nesses termos. Neste sentido, cfr. CARLOS RODRIGUES DE ALMEIDA, "O registo de som e imagem…", cit., p. 376
[176] JOÃO GOUVEIA CAIRES, "Métodos ocultos na criminalidade económico-financeira…", cit., p. 52

lealdade processual[177], não o faz de forma mais onerosa para o arguido do que outros métodos que encontramos na nossa lei.

Assim, reconhecendo que, além dos direitos fundamentais analisados mais aprofundadamente, também o recurso a este tipo de técnicas contende com direitos fundamentais adjetivos[178], entendemos que, essencialmente por razões de economia do presente texto, não cumprirá fazer uma análise mais detalhada desta problemática.

Ademais, pretendemos apenas deixar nota de que na análise da gravidade deste tipo de técnicas não se pode igualmente ignorar a sua potencialidade para afetar todos aqueles direitos referidos do arguido, mas igualmente de terceiros[179]. Isto contribui para a caracterização deste meio como extremamente invasivo, e deve necessariamente contribuir para a delimitação do seu regime legal. Podendo afirmar-se que o sistema processual penal convive com a possibilidade de afetação de direitos fundamentais de terceiros[180], em circunstâncias pontuais e particulares, essa circunstância deve manifestar-se, por exemplo, quanto aos requisitos de admissibilidade e formalidades de execução da diligência, com intuito de proteger terceiros afetados pela mesma.

2.3. UTILIZAÇÃO DE *MALWARE* COMO MÉTODO DE OBTENÇÃO DE PROVA EM ORDENAMENTOS JURÍDICOS ESTRANGEIROS

A problemática acerca da utilização de *malware* no seio de investigações criminais não é exclusiva ao ordenamento jurídico nacional, uma vez que os impactos da evolução tecnológica no combate à criminalidade se fazem sentir em termos globais. Na verdade, vários Estados já se confrontaram com o recurso a meios deste tipo, trazendo ao debate as problemáticas suscitadas, e adaptando a sua legislação às novas realidades. Entendemos que a análise sucinta dos regimes vigentes noutros países pode contribuir para o estudo do problema no nosso ordenamento jurídico, uma vez que nos permitirá

---

[177] DAVID SILVA RAMALHO, "A investigação criminal na Dark web…", cit., p. 417

[178] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…",* cit., p. 106

[179] MANUEL DA COSTA ANDRADE, "Métodos ocultos…", cit., p. 536; JULIANA SOUSA CAMPOS, *O Malware…*, cit., p. 65

[180] O regime legal das escutas telefónicas evidencia que as mesmas atingem «a esfera jurídica de pessoas que estão fora do círculo dos arguidos e suspeitos (…). O que pode abrir porta à devassa da privacidade de pessoas a que (…) a lei outorga o direito (…) de recusa de depoimento» cfr. MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova…,* cit., pp. 290-291. Sem pretensão de exaustividade em relação a esta temática, pretendemos apenas deixar claro que, do mesmo modo que o regime das escutas se coaduna necessariamente com a afetação de direitos de terceiros, tal poderá suceder igualmente no que concerne à utilização de técnicas de *malware*.

analisar as soluções encontradas para conciliar o sucesso da investigação criminal com os direitos fundamentais e garantias processuais do arguido.

De seguida, analisaremos então o regime vigente nos Estados Unidos, em Espanha e na Alemanha no que concerne à utilização de *malware* como método de investigação. Sendo certo que não são os únicos países cuja legislação regula a utilização de *malware*, para efeitos do presente texto entendemos que o estudo dos mesmos permite uma análise simultaneamente sucinta e aprofundada da problemática. No que concerne aos Estados Unidos, este país foi pioneiro no que diz respeito à utilização de *malware* pelas autoridades de investigação; já no que diz respeito à análise dos regimes espanhol e alemão, trata-se de sistemas jurídicos muito próximos do nosso, que se encontram, no âmbito desta matéria, um passo à frente, na medida em que regulam expressamente a utilização de *malware* no âmbito de investigações criminais.

2.3.1. Regime nos EUA

O recurso ao *malware* pelas autoridades de investigação criminal nos Estados Unidos data, pelo menos, a 1999[181], e tem desde então feito parte da prática judiciária. Tendo começado com a instalação física de *keyloggers* no dispositivo do visado[182], foi posteriormente desenvolvida uma tecnologia a que se chamou *Magic Lantern*, que permitia igualmente acesso às teclas premidas no dispositivo, mas diferia da anterior na medida em que poderia ser instalada remotamente[183]. A esta técnica seguiu-se o CIPAV (*Computer and Internet Protocol Address Verifier*) que permite às autoridades aceder ao endereço IP que estaria inacessível em virtude da utilização do TOR[184], tendo sido posteriormente superada pela NIT (*network invesitgative technique*), que mais não é do que uma versão mais recente do *software* utilizado pelo FBI[185]. Tendo a nomeação de cada destes programas sido alterada em função da sua evolução, trata-se, no fundo, de

[181] Sayako Quinlan / Andi Wilson, *A brief history of law enforcement hacking in the United States,* Cybersecurity Initiative, 2016, p. 3, disponível em: https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf (consultado a 22/3/2023)
[182] *Ibidem*
[183] Christopher Woo / Miranda So, "The case for magic lantern: September 11 highlights the need for increased surveillance", in *Harvard Journal of Law & Technology*, volume 15, number 2, 2002, p. 524, disponível em: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf (consultado a 22/3/2023)
[184] Sayako Quinlan / Andi Wilson, *A brief history of law enforcement hacking in the United States…,* cit., p. 6
[185] *Ibidem*

técnicas de *hacking* por parte das autoridades que permitem o acesso remoto e oculto aos dados contidos num dispositivo[186].

Neste ordenamento jurídico, o obstáculo principal que se verificou no recurso ao *malware* prendeu-se essencialmente com aspetos formais no que concerne aos mandados de busca que autorizavam a utilização de técnicas de *malware*. A maioria dos mandados eram ordenados ao abrigo da regra 41 das FRCP, mas a redação anterior desta regra originava um obstáculo de jurisdição nas situações em que não se tivesse conhecimento da localização do dispositivo a que se pretendia aceder[187]. Com o intuito de fazer frente aos desafios da cibercriminalidade e de modo a facilitar o recurso a este tipo de meios técnicos de investigação pelas autoridades[188], foi a regra 41 alterada em 2016, permitindo-se agora na regra 41(6) a emissão de mandados de busca para acesso remoto a dispositivos eletrónicos quando (a) a sua localização tenha sido ocultada por via de meios eletrónicos ou (b) perante o cometimento de determinados crimes, determinados computadores tenham sido alvo de ataque informático. Assim, foi eliminado aquele que era o maior obstáculo à emissão de mandados de busca que autorizassem a utilização de *malware.*

Previamente a estas alterações, havia quem defendesse que a autorização de recurso a este tipo de buscas deveria estar sujeita às regras do *Wiretap Act*, em virtude do seu grau de invasividade[189], uma vez que aquele diploma exige a verificação de requisitos mais apertados para autorização das medidas, oferecendo assim maiores garantias. Não obstante, atenta a nova letra da regra 41 das FRCP, é com base no procedimento aí previsto que se autoriza a utilização de *malware.*

No que concerne aos requisitos que têm de se verificar para ser admissível a utilização de *malware*, terá de se observar os requisitos de "causa provável" e "particularidade", impostos pela Quarta Emenda da Constituição dos Estados Unidos para

---

[186] RICHARD M. THOMPSON II, "Digital searches and seizures: overview of proposed amendments to rule 41 of the rules of criminal procedure", 2016, p. 2, disponível em: https://sgp.fas.org/crs/misc/R44547.pdf (consultado a 22/3/2023)

[187] *Ibidem*, p. 4

[188] DEVIN M. ADAMS, "The 2016 amendments to criminal rule 41: national search warrants to seize cyberspace, "particularly" speaking", *University of Richmond Law Review*, vol. 51, 2017, p. 728, disponível em: https://scholarship.richmond.edu/law-student-publications/146/#:~:text=Rule%2041%2C%20governing%20searches%20and%20seizures%2C%20now%20permits,devices%20in%20multiple%20districts%20anywhere%20in%20the%20country (consultado a 22/3/2023)

[189] RICHARD M. THOMPSON II, "Digital searches and seizures:…", cit., p. 8

a emissão de qualquer mandado de busca[190]. Donde, sendo um mandado que autorize as buscas remotas emitido ao abrigo da regra 41(6)(a), a sua emissão dependerá sempre da verificação daqueles dois requisitos, e nunca a sua admissibilidade decorrerá da mera ocultação através de meios tecnológicos[191]. Assim, o requerente terá de invocar "factos suficientes" que permitam ao juiz concluir pela probabilidade de que a busca levará à obtenção de prova[192], e terá de identificar o alvo da busca. No que concerne ao requisito da "particularidade", a verificação do mesmo pode ser obstada pela utilização de anonimizadores, o que dá azo a críticas e dúvidas[193].

Ao contrário do que se verificará nos ordenamentos jurídicos espanhol e alemão, não se impõe aqui qualquer catálogo de crimes em relação à investigação dos quais é admissível a utilização de *malware.* Quanto ao tipo de *malware* permitido, é certo que parece decorrer da redação da regra 41 que os mandados aí regulados se destinam à recolha de prova interna, o que nos levaria a excluir a obtenção de prova externa – no entanto, quanto a esse aspeto, fica a questão de possibilidade de utilização dos *keyloggers.*

2.3.2. Regime em Espanha

No ordenamento jurídico espanhol, até à entrada em vigor da Lei Orgânica 13/2015, discutia-se a admissibilidade de utilização de *malware* no âmbito da investigação criminal, propugnando-se pela alteração da LECrim de modo a regular as novas possibilidades técnicas trazidas pela evolução tecnológica[194]. Em virtude da adoção da referida lei, e procurando dar cumprimento às recomendações europeias acerca da investigação do cibercrime[195], foi introduzido o artigo 588 *septies* que prevê e regula, nas

---

[190] Mark Rumold, "Assessing the legality and proportionality of communications surveillance in United States law", 2016, p. 13, disponível em: https://necessaryandproportionate.org/files/us-en-march2016.pdf (consultado a 22/3/2023)

[191] Markus Rauschecker "Rule 41 amendments provide for a drastic expansion of government authority to conduct computer searches and should not have been adopted by the supreme court", *Maryland Law Review,* volume 76, issue 4, 2017, p. 1094, disponível em: https://digitalcommons.law.umaryland.edu/mlr/vol76/iss4/8/ (consultado a 22/3/2023)

[192] Mark Rumold, "Assessing the legality and proportionality of communications surveillance…"; cit., p.13

[193] Markus Rauschecker "Rule 41 amendments provide for a drastic expansion of government authority…", cit., p. 1093

[194] Juan Carlos Ortiz Pradillo, "«Hacking» legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática", *Revista de Derecho y Proceso Penal*, nº26, Aranzi, 2011, p. 78; Inmaculada López-Barajas Perea, "Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos" in *Revista de Internet, Derecho y Política*, nº24, fevereiro, 2017, p. 66, disponível em: https://www.redalyc.org/articulo.oa?id=78850913006 (consultado a 22/3/2023)

[195] Lorena Bachmaier Winter "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015" in *Boletín del Ministerio de Justicia*, año LXXI, numero 2195, enero de 2017,

alíneas a) a c), o *registro remoto de equipos informáticos* através da utilização de dados de identificação e códigos, ou por via de instalação de um *software,* concretamente, cavalos de Tróia[196]. Ademais, é orientação da doutrina que também se deverá autorizar, ao abrigo deste artigo, a utilização de *keyloggers*[197]. Ao referir-se expressamente à instalação sub-reptícia num determinado sistema informático de um *software* que permite a monitorização da atividade e registo e cópia, e posterior reenvio às autoridades, dos dados contidos nesse sistema[198], não restam dúvidas de que se consagra a utilização de *malware* no âmbito da investigação criminal.

A regulação deste método de prova obedece às disposições específicas do artigo 588 *septies*, mas também às disposições gerais aplicáveis às medidas tecnológicas do artigo 588 *bis*. Do disposto nestes artigos resulta, desde logo, que a admissibilidade de recurso a este método de investigação se encontra restringida a um catálogo de crimes (artigo 588 *septies* a.), ao contrário do que sucede nos Estados Unidos. Contudo, a seleção de crimes operada pelo legislador tem sido alvo de críticas por parte da doutrina[199]. Sendo os *registros remotos de equipos informáticos* autorizados em relação à investigação de crimes graves (p.e., delitos cometidos no âmbito de criminalidade organizada e crimes de terrorismo), a al. e) do artigo 588 *septies* a. (1) estende essa admissibilidade a crimes cometidos através de sistemas informáticos, independentemente da gravidade, colocando em crise o princípio da proporcionalidade[200].

Por outro lado, a admissibilidade deste método de investigação encontra-se dependente de autorização judicial, nos termos do artigo 588 *bis* b. (1), a qual poderá ser oficiosa ou requerida pelo Ministério Fiscal ou pela Policia Judicial através de requerimento que observe os requisitos do artigo 588 *septies* a. (2), impondo ainda o artigo 588 *bis* a. expressamente o respeito pelos princípios da especialidade, idoneidade, excecionalidade, necessidade e proporcionalidade, aquando da autorização da medida.

---

p. 33, disponível em: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=R3jUJW0AAAAJ&citation_for_view=R3jUJW0AAAAJ:4OULZ7Gr8RgC (consultado a 22/3/2023)

[196] PALOMA ARRABAL PLATERO "Las diligencias de investigación tecnológica en el proceso penal español", in *Revista de Ciencias Sociales*, numero 76, 2020, p. 99, disponível em: https://www.researchgate.net/publication/367939659_Las_diligencias_de_investigacion_tecnologicas_en_el_proceso_penal_espanol (consultado a 22/3/2023)

[197] Ibidem, p. 99; ISIDORO ESPÍN LÓPEZ, *Investigación sobre equipos informáticos y su prueba en el proceso penal*, Aranzadi, 2021, p. 192

[198] JULIANA SOUSA CAMPOS, *O Malware…,* cit., p. 108

[199] JULIANA SOUSA CAMPOS, *O Malware…*, cit., p. 116; LORENA BACHMAIER WINTER, "Registro remoto…", cit., p. 15; ISIDORO ESPÍN LÓPEZ, *Investigación sobre equipos informáticos…,* cit., pp. 200 e ss.

[200] ISIDORO ESPÍN LÓPEZ, *Investigación sobre equipos informáticos*…, cit., p. 203

Além disso, o artigo 588 *septies* c. regula a duração da medida e possibilidade de prorrogação da mesma.

Uma outra questão suscitada pela doutrina espanhola prende-se com aferir se a lei permite apenas o acesso a dados armazenados, ou também a dados produzidos em tempo real[201]. Embora a letra da lei se refira a "dados armazenados" e "ao conteúdo do dispositivo"[202], o artigo 588 *septies* a. (1) refere-se expressamente à instalação de *software*, o que permitirá a monitorização da atividade e acesso aos dados produzidos em tempo real[203], pelo que se discute a admissibilidade desta técnica para proceder à interceção de comunicações[204]. Tem-se entendido, e em nossa opinião, corretamente, que o propósito do legislador, através da regulação destas "buscas remotas", não terá sido regular a interceção de comunicações[205]. Donde, quando esteja em causa a interceção de comunicações deverá recorrer-se ao artigo 588 *ter*.

Posto isto, pode verificar-se que a lei espanhola opera uma regulação extensa e detalhada da utilização deste tipo de técnicas no âmbito da investigação criminal, ainda que lhe sejam apontadas algumas críticas[206].

2.3.3. REGIME NA ALEMANHA

Embora o debate acerca da utilização de *malware* como método de investigação se tenha iniciado cedo[207], foi através da lei de 17-08-2017 que foi consagrado no StPO, com o intuito de tornar os processos criminais mais eficazes[208]. Em contraste com os ordenamentos anteriormente analisados, a utilização de *malware* foi consagrada em dois

---

[201] LORENA BACHMAIER WINTER, "Registro remoto…", cit., p. 13
[202] JULIANA SOUSA CAMPOS, *O Malware…,* cit., p. 123
[203] ISIDORO ESPÍN LÓPEZ, *Investigación sobre equipos informáticos*…, cit., p. 194
[204] *Ibidem*, pp. 206 e 207
[205] *Ibidem*, p. 206; LORENA BACHMAIER WINTER "Registro remoto…", cit., p. 15
[206] LORENA BACHMAIER WINTER "Registro remoto…", cit., p. 33
[207] Como vimos em capítulo anterior, em fevereiro de 2008 o BVerfG emitiu uma decisão no âmbito da fiscalização da conformidade constitucional do §5(2) n.º11 a Lei de Proteção da Constituição da Renânia do Norte-Vestefália, abordando a problemática da infiltração oculta em sistemas informáticos. Posteriormente, em dezembro de 2008, foi aprovada a Lei de defesa contra os perigos do terrorismo internacional através da Polícia Judiciária federal, a qual previa «meios de vigilância nas telecomunicações, inclusive a intervenção encoberta em sistemas informáticos (a chamada *busca online*)», os quais se tratavam «não de meios de prossecução penal, mas sim de defesa contra perigos e de prevenção de crimes», cfr. KLAUS ROGALL, "A nova regulamentação da vigilância das telecomunicações na Alemanha", in *2.º Congresso de Investigação Criminal* (coord. Maria Fernanda Palma, et al.), Coimbra, Almedina, 2011, pp. 120 e 121. Nesta conjetura, discutia-se a admissibilidade da vigilância na fonte das telecomunicações, através da instalação de um *software*, no âmbito do processo penal, cfr. KLAUS ROGALL, "A nova regulamentação…", cit., pp. 125 e 126
[208] ARTHUR HARTMANN, „§100a", in *Gesamtes Strafrecht Kommentar, StGB / StPO / Nebengesetze – Handkommentar*, (ed. Dieter Rössner), 5ª ed., Nomos, 2022, p. 2316

preceitos diferentes, tratando-se de medidas com finalidades distintas. Por um lado, a secção §100a, parágrafo 1, prevê a *Quellen-TKÜ*, que consiste na vigilância das telecomunicações na fonte, permitindo monitorizar telecomunicações encriptadas no terminal da telecomunicação do remetente (antes da encriptação) ou do destinatário (depois da desencriptação)[209]. Assim, estabelece-se uma base legal para a vigilância na fonte, permitindo a monitorização de comunicações que não podem ser intercetadas através dos métodos convencionais. Por outro lado, a revista secção §100b passou a consagrar as *Online-Durchsuchung* (buscas *online*), regulando o acesso oculto a sistemas de tecnologia de informação, permitindo o acesso e recolha dos dados aí armazenados[210]. Assim, perante as várias funcionalidades permitidas pela utilização de *malware*, o legislador alemão previu a sua utilização para medidas diversas.

Residindo a principal diferença entre as duas medidas nos direitos concretamente afetados e tutela constitucional conferida[211], do ponto de vista técnico, o *malware* utilizado é semelhante[212] e em ambos os casos as medidas encontram-se sujeitas a um catálogo de crimes e às disposições das secções §100d e §100e, as quais regulam os limites impostos às diligências em virtude da proteção da área nuclear da vida privada e do direito de recusa de depoimento (§100d), e os requisitos formais e procedimentos a observar no exercício das medidas (§100e). Tanto a secção §100a (1), n.º1, como a secção §100b (1), n.º1, se referem a "crimes graves", sendo este conceito densificado, respetivamente, no parágrafo (2) de cada uma das mencionadas secções, estando a admissibilidade da diligência dependente da verificação em concreto da gravidade do crime (§100a (1), nº2 e §100b (1), n.º2). Por outro lado, em ambos os casos restringe-se, em princípio, a diligência ao arguido, apesar de nas *Quellen-TKÜ* ser admissível que o visado seja outra pessoa desde que haja fundadas suspeitas de que se encontra a comunicar com o arguido ou que o arguido se está a fazer valer do seu dispositivo. No

---

[209] ARTHUR HARTMANN, „§100a"…, cit., p. 2316

[210] *Ibidem*, p. 2331

[211] Enquanto as *Quellen-TKÜ* representam uma intromissão no âmbito de proteção do direito à privacidade das telecomunicações, nos termos do artigo 10.º da Constituição Federal Alemã, as *Online-Durchsuchung* permitem o acesso a dados que caem na esfera de tutela do direito fundamental à integridade e confidencialidade dos sistemas informáticos. ARTHUR HARTMANN, „§100a"…, cit., p. 2324; MARCUS KÖHLER, „§100b", in *Strafprozessordnung: Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen*, Beck'rcheKurz-Kommentare (Bertram Schmitt & Marcus Köhler), 64ª ed., Munique, C.H.Beck, 2021, p. 425

[212] DIETER KOCHHEIM, "Onlinedurchsuchung und Quellen-TKÜ in der Strafprozessordnung – Neuordnung der tiefen technischen Eingriffsmaßnahmen in der StPO seit dem 24.8.2017", 2018, p. 62, disponível em: https://kripoz.de/wp-content/uploads/2018/03/kochheim-onlinedurchsuchung-und-quellen-tkue-in-der-stpo.pdf (consultado a 22/3/2023)

caso das *Online-Durchsuchung*, a lei é explícita sobre a admissibilidade da diligência mesmo no caso de terceiros poderem ser afetados pela mesma, em certas circunstâncias. Ademais, ambas as diligências se encontram sujeitas a uma expressa cláusula de subsidiariedade, e carecem de autorização judicial.

Estando em causa a instalação de um *software* no dispositivo do visado, a lei, na secção §100a (5) (para a qual remete a secção §100b (4)) estabelece determinados requisitos técnicos que têm de se verificar para admissibilidade da diligência, e que visam, no fundo, limitar a interferência na privacidade do visado. Nomeadamente, estabelece-se que o *software* deve ser desenvolvido de modo a proteger o sistema contra a utilização não autorizada e os dados copiados contra modificações, apagamento e divulgação não autorizados[213].

Como foi referido, as *Quellen-TKÜ* destinam-se a permitir a vigilância de telecomunicações na fonte, e, portanto, permitem o acesso aos dados de conteúdo e aos metadados que seriam admissíveis caso tivesse sido possível recorrer à vigilância tradicional, e as *Online-Durchsuchung* permitem o acesso a dados armazenados num determinado sistema. Donde, está, em princípio, vedada a utilização de *malware* para recolha de prova externa, através do acesso ao microfone e/ou à câmara[214]. No entanto, a secção §100c e §100f aludem à utilização de "meios técnicos" para gravação da palavra falada, sem o conhecimento da pessoa, e tem-se entendido que é admissível fazer uma vigilância acústica através do acesso a um sistema de informação nos termos do §100b[215]. Assim, nesse entendimento, parece-nos que será admissível a recolha de prova externa, i.e. voz[216].

À semelhança da lei espanhola, entendemos que o ordenamento jurídico alemão apresenta uma regulação extensa e detalhada da utilização de *malware* no âmbito do processo penal. Em bom rigor, dos ordenamentos analisados, é aquele que nos parece mais adequado, essencialmente por se reconhecer que o recurso a técnicas de *malware* pode afigurar-se útil no âmbito de diferentes diligências.

Desta breve análise acerca da utilização de *malware* enquanto método de investigação noutros ordenamentos jurídicos resulta uma preocupação em sujeitar estas

[213] ARTHUR HARTMANN, „§100a"…, cit., p. 2326
[214] MARCUS KÖHLER, „§100b"…, cit., p. 426
[215] ARTHUR HARTMANN, „§100a"…, cit., p. 2332
[216] JULIANA SOUSA CAMPOS, *O Malware…,* cit., p. 125

medidas a determinados requisitos[217], assegurando a adequação constitucional da utilização deste tipo de técnicas. Em todos os casos, não se ignora os riscos do recurso a este tipo de técnicas, nem o seu grau de danosidade e intrusão na privacidade dos visados[218], estabelecendo-se requisitos *ex ante* e mecanismos *ex post* que assegurem a proporcionalidade e necessidade da utilização deste tipo de técnicas[219].

[217] Tanto no que concerne à admissibilidade da medida, mas também relativamente ao controlo sobre a execução da mesma, apesar de, por questões de economia do texto, não nos termos referido detalhadamente a todos.
[218] MIRJA GUTHEIL / QUENTIN LIGER / AURÉLIE HEETMAN / JAMES EAGER / MAX CRAWFORD, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices", Study for de LIBE Committee, 2017, p. 67, disponível em: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2017)583137 (consultado a 27/12/2022)
[219] *Ibidem*

3. ADMISSIBILIDADE DE *MALWARE* COMO MÉTODO DE OBTENÇÃO DE PROVA À LUZ DA LEI PROCESSUAL PENAL PORTUGUESA

A discussão sobre a utilização de *malware* como método de obtenção de prova tem vindo a ser suscitada, no seio da doutrina nacional, em anos recentes, sendo possível encontrar opiniões divergentes relativamente à conformidade legal deste método de obtenção de prova, e entre os autores apologistas de que a lei portuguesa prevê o *malware* ou as buscas *online*, não existe um consenso relativamente à base legal da sua previsão. Efetivamente, enquanto existe quem defenda que a lei portuguesa prevê as buscas *online* (nas quais, como vimos, se enquadra a utilização de *malware*) na redação do artigo 15.º LCC[220], outros autores encontram a base legal em que se fundamenta a admissibilidade do *malware* na previsão do n.º2 do artigo 19.º LCC[221]. Outros ainda propugnam pela aplicação do regime do artigo 18.º LCC[222].

Perante as diversas opiniões avançadas pela doutrina portuguesa nesta matéria, entendemos que, numa tentativa de as agrupar, seria possível defender a existência de: a) uma solução alargada, na medida em que se defende que as buscas *online* estão previstas quase incondicionadamente, nos termos do artigo 15.º LCC; b) soluções intermédias, que restringem a admissibilidade deste método de obtenção de prova à verificação de determinados requisitos; c) uma solução restrita, que rejeita a admissibilidade deste método de obtenção de prova no ordenamento jurídico português por ausência de previsão legal expressa[223].

De seguida, iremos analisar cada uma destas posições e respetivos argumentos. No entanto, veremos que qualquer das soluções, com exceção da mais restrita, são, em nosso entendimento, indefensáveis, porque sempre se chega à conclusão de

---

[220] TIAGO CAIADO MILHEIRO, "Buscas online" in *Corrupção em Portugal: avaliação legislativa e propostas de reforma* (org. Paulo Pinto de Albuquerque, et al.), Lisboa, Universidade Católica Editora, 2021, p. 558; PAULO PINTO DE ALBUQUERQUE, *Comentário ao Código de Processo Penal*…, cit., p. 502; DUARTE RODRIGUES NUNES, *O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada*, 1ª ed., Coimbra, Gestlegal, 2019, p. 812

[221] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 338; JOÃO CONDE CORREIA, "Prova Digital…", cit., p. 43

[222] DUARTE RODRIGUES NUNES, *O problema da admissibilidade…,* cit., p. 812

[223] JULIANA SOUSA CAMPOS, *O malware…,* cit., pp. 101 e 102; DANIEL BENTO ALVES, "Uso de *malware* em investigação criminal" in *Actualidad Jurídica Uría Menéndez*, 2017, pp. 28 e ss., disponível em: https://www.uria.com/documentos/publicaciones/5655/documento/AJUM-47-001.pdf?id=7642&forceDownload=true (consultado a 19/10/2022); MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…"* cit., pp. 165-169; BENJAMIM SILVA RODRIGUES, *Da Prova Penal…,* cit., pp. 379 e 380; SÓNIA FIDALGO, "A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo" in *A Inteligência Artificial no Direito Penal* (coord. Anabela Miranda Rodrigues), reimpressão, 2022, pp. 153-154

inconstitucionalidade dos preceitos mencionados, quando interpretados no sentido de admitirem a utilização de *malware*. Ademais, entendemos que tais soluções pecam, na sua maioria, por entenderem o *malware* como um todo, enquanto método de obtenção de prova, ao invés de tomarem em consideração as específicas funcionalidades colocadas à disposição por este tipo de técnicas informáticas. Em bom rigor, entendemos que encarar o *malware* como um método de prova único em si e como um todo não configura a abordagem mais correta e adequada do problema, uma vez que atendendo àquilo para que o *software* pode ser programado, a questão deveria ser colocada do ponto de vista de quais os métodos de obtenção de prova já existentes que podem ser complementados pela utilização de *malware* e que outros métodos carecem ainda de ser previstos. Na verdade, na doutrina, aqueles que se referem à utilização de *malware*, parecem entendê-lo como um todo; enquanto quem se refere separadamente às buscas *online* e à vigilância na fonte oferece um tratamento diferenciado a ambas, apesar de num e noutro caso se pressupor a utilização de *malware*. No fundo, como veremos, trata-se de uma matéria cuja abordagem, no seio da doutrina, não é consistente e diríamos que é, no limite, confusa. Já do lado da jurisprudência nacional, o tratamento é inexistente. Donde, a análise desta problemática no âmbito do ordenamento jurídico português apresenta diversos desafios.

Antes de partir para uma análise crítica e detalhada das diversas opiniões existentes, e retomando o que explicámos anteriormente acerca da diversidade de conceitos utilizados na doutrina para abordar esta temática[224], cumpre fazer uma outra ressalva relativamente à diferença entre buscas *online* e *malware*. Ambos os termos são, por vezes, utilizados indiscriminadamente para descrever a mesma realidade, no entanto, há quem distinga os dois. Conforme clarificámos anteriormente, alguns autores[225] referem-se ao termo «buscas *online*» no pressuposto de que este compreende o termo «*malware*», enquanto outros autores[226] os distinguem, não podendo valer o que defendem quanto à admissibilidade das buscas *online* para defesa da admissibilidade da utilização de *malware.* É, porém, de notar que apenas TIAGO CAIADO MILHEIRO parece fazer esta distinção estanque, defendendo que as ditas buscas *online* consistem em diligências realizadas de forma contínua e num período temporal circunscrito, para aceder a dados armazenados[227], opondo-as assim ao *malware,* que se prolonga no tempo e permite o

[224] *Vide*, pp. 14 e 15 do presente texto
[225] PAULO PINTO DE ALBUQUERQUE, *Comentário ao Código de Processo Penal*…, cit., p. 502;
[226] TIAGO CAIADO MILHEIRO, "Buscas online"…, cit., p. 561
[227] *Ibidem*, p. 561

acesso a dados em tempo real. Este autor defende sem qualquer dúvida a admissibilidade das buscas *online*, comparando-as às pesquisas de dados informáticos, no entanto, a restante doutrina, ao referir as buscas *online* não faz esta distinção em relação ao *malware*, utilizando o termo para descrever variadas realidades. Na economia do presente estudo, pretendemos apenas deixar claro que circunscrevemos a nossa análise, às posições doutrinárias que se refiram, expressamente ou não, à utilização de *malware*.

3.1. SOLUÇÃO ALARGADA: O ARTIGO 15.º LCC

Sufragada por PAULO PINTO DE ALBUQUERQUE[228] e DUARTE RODRIGUES NUNES[229], ainda que em termos distintos, esta orientação vai de encontro à admissibilidade da utilização de *malware* como método de obtenção de prova previsto no artigo 15.º LCC. PAULO PINTO DE ALBUQUERQUE defende que a busca *online* se traduz «na infiltração electrónica em sistemas informáticos, por exemplo, através dos chamados cavalos de Tróia, de modo a que o investigador possa em tempo real ou deferido conhecer a informação que está a ser introduzida ou já foi introduzida no sistema.»[230], sufragando que as mesmas foram introduzidas expressamente na lei portuguesa através do artigo 15.º LCC.

O autor não desenvolve aprofundadamente os argumentos que o levam a considerar que as buscas *online*, abarcando a utilização de *malware*, se encontram previstas no artigo 15.º LCC[231], pelo que não nos é possível dissecar os mesmos com vista a refutá-los. Não obstante, PAULO PINTO DE ALBUQUERQUE reconhece que este método comporta um grau extraordinário de intrusão na privacidade do visado, tendo de ser regulado por uma lei expressa e devendo exigir reserva de competência judicial[232]. Ora, o autor admite que «a lei não coloca quaisquer restrições relativamente aos conteúdos dos dados que podem ser pesquisados (…)»[233] e que «a lei nova também não exige que a pesquisa informática ordenada pelo MP ou pelo OPC seja validada pelo juiz (…)», concluindo que assim o preceito sob análise seria inconstitucional[234]. Ora, salvo melhor opinião, temos muita dificuldade em aceitar este pensamento do autor.

---

[228] PAULO PINTO DE ALBUQUERQUE, *Comentário ao Código de Processo Penal*…, cit., p. 502
[229] DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova…,* cit., pp. 226 e ss.
[230] *Ibidem*
[231] PAULO PINTO DE ALBUQUERQUE, *Comentário ao Código de Processo Penal*…, cit., p. 502
[232] *Ibidem*
[233] *Ibidem*
[234] *Ibidem*

Efetivamente, do que se trata é de tentar, por via interpretativa, incluir o *malware* na previsão de um preceito legal que não o prevê expressamente, para concluir que se está perante uma inconstitucionalidade material, precisamente por se tratar de um método extremamente invasivo com um potencial lesivo de direitos fundamentais, pelo que tem de ser expressa e cuidadosamente regulado. A letra do artigo 15.º LCC não se refere expressamente à utilização de *malware*, e reconduzir as buscas *online*, na aceção já explicada, a este artigo leva, inevitavelmente, à conclusão sobre a inconstitucionalidade do mesmo. De todo o modo, a conclusão sobre a inconstitucionalidade do artigo interpretado nesse sentido pressupõe que se reconduza a base legal do *malware* ao mesmo, o que, em nosso entender, não é de acolher.

Desde logo, a letra do artigo 15.º LCC refere-se ao acesso a «dados (…) *armazenados*[235] num determinado sistema informático», o que exclui necessariamente a obtenção de dados produzidos em tempo real ou dados não armazenados no sistema. Ora, como vimos, a utilização de *malware* permite a monitorização da atividade desenvolvida num determinado sistema, e até a eventual recolha de prova externa. Efetivamente, a utilidade e eficácia do recurso ao *malware* no âmbito das investigações criminais reside maioritariamente nas possibilidades que este tipo de técnicas oferecem à investigação, as quais vão muito para além do mero acesso a dados armazenados num determinado sistema. Quanto a este ponto, DUARTE RODRIGUES NUNES divide a sua análise entre os casos em que a diligência consiste num único acesso ao sistema e aos dados aí armazenados (*Daten-Spiegelung*)[236] e aqueloutros em que ocorra um acesso contínuo e prolongado no tempo, permitindo o acesso aos dados produzidos em tempo real e uma monitorização de toda a atividade desenvolvida no sistema, incluindo acessos à *internet* (*Daten-Monitoring*)[237]. Segundo este autor, as buscas *online*, independentemente da sua modalidade, estão previstas no artigo 15.º LCC, sendo que a diferença reside no regime jurídico aplicável[238]. A primeira modalidade de acesso estaria sujeita ao regime previsto no mesmo artigo, em virtude de se tratar de um acesso em tudo semelhante ao da pesquisa de dados informáticos[239], ao passo que os casos de *Daten-Monitoring* deveriam ser submetidos ao regime do artigo 18.º LCC, em virtude de possuírem uma danosidade

[235] Itálico nosso
[236] DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova…,* cit., p. 227
[237] *Ibidem*, p. 231
[238] *Ibidem*, p. 234
[239] *Ibidem*

semelhante à das intervenções nas comunicações[240]. Admitindo que, ao contrário da maioria da doutrina, o autor reconhece que a infiltração oculta em sistemas informáticos pode comportar graus distintos de danosidade e afetação de direitos fundamentais, sendo inadequado a procura por um regime unitário, não podemos deixar de discordar da solução avançada. Desde logo, a aplicação analógica do regime da interceção de comunicações deverá ser evitada, por proibida, nos termos expostos supra[241]. Além disso, o artigo 15.º LCC não pode servir de base legal a qualquer das modalidades de buscas *online* apresentadas pelo autor. Sendo evidente que nada na letra da lei indica a previsão de um método que autorize o acesso a dados produzidos em tempo real ou não armazenados, mesmo no caso de *Daten-Spiegelung*, que mais se aproxima à pesquisa de dados informáticos no que concerne ao acesso a dados armazenados, temos dúvidas sobre a sua subsunção a este artigo.

A letra do artigo 15.º LCC, além de referir dados armazenados, refere-se à «pesquisa de dados *específicos e determinados*[242]», os quais, necessariamente, terão de se relacionar com os factos em investigação e respetiva prova[243]. Sendo certo que com a utilização de *malware* não se pretende admitir a pesquisa ou busca indeterminada, carecendo sempre de justificação que se relacione com a obtenção de informação relevante para a investigação, a mesma permitirá o acesso a inúmeros dados. Perante a impossibilidade técnica de restringir, através da programação do *software,* o acesso a determinados dados[244], o controlo de quais os dados relevantes e admissíveis para o processo far-se-á *a posteriori*, (à semelhança do regime das escutas telefónicas), sendo que o recurso ao *malware* deverá estar sujeito à indispensabilidade ou grande necessidade da medida, e à convicção de que com a mesma se acederá a informações relevantes para o processo (à semelhança do que sucede noutros regimes jurídicos), e deverá acautelar-se que o *software* utilizado permite apenas o grau de intrusão necessário à eficácia da diligência[245]. Não obstante, a exigência de que esteja em causa a pesquisa de dados específicos e determinados leva-nos desde logo a crer que tal desiderato não é compatível com a utilização de *malware*, até porque a utilização de *malware* se pode prender

[240] DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova…,* cit., pp. 231 e 234
[241] *Vide*, capítulo 1
[242] Itálico nosso
[243] RUI COSTA PEREIRA, "A pesquisa de dados informáticos", in *Revista Portuguesa de Ciência Criminal,* ano 31, nº3, setembro-dezembro 2021, p. 586
[244] BENJAMIM SILVA RODRIGUES, Da Prova Penal…, cit., p. 379
[245] À semelhança do que se verifica noutros ordenamentos jurídicos, cfr. §100a (5) StPO

precisamente com o facto de não ser possível determinar, previamente à execução da medida, quais os dados a que se pretende aceder e apreender. Ademais, apesar de a *praxis* no nosso ordenamento jurídico assentar nas «pesquisas cegas»[246], que consistem na busca, no âmbito do sistema informático, dos dados através de palavras-chave que se relacionam com o objeto do processo, tal prática dificilmente se reconduz à determinabilidade e especificidade exigidas pela norma[247], uma vez que, restringindo o objeto da pesquisa e garantindo uma maior eficiência da investigação, não impedem que se aceda a dados irrelevantes para o processo, nem tão-pouco a possibilidade de conhecimentos fortuitos[248]. Sem pretensão de entrar em detalhe no debate acerca da admissibilidade das pesquisas por palavras-chave, ponto é que havendo dúvidas acerca da sua conformidade com o disposto no artigo 15.º LCC em virtude da exigência de «dados específicos e determinados», então dúvidas ainda maiores existirão acerca da admissibilidade do *malware* nos termos deste preceito.

Por outro lado, o *malware* é um método cuja utilidade reside precisamente no seu caráter oculto de infiltração num sistema informático. Ora, não só não resulta do regime sob análise qualquer elemento que indicie a infiltração prévia no sistema[249], como a diligência prevista no artigo 15.º LCC será tendencialmente uma medida aberta, efetuada com o conhecimento do visado[250]. O n.º 6 do artigo 15.º LCC remete para o regime das de execução das buscas previsto no CPP, concretamente no artigo 176.º[251]. Ora, as buscas físicas são um método de obtenção de prova aberto, que permite ao visado assistir à diligência[252], tendo a oportunidade de controlar a sua execução e respetivos limites, e até entregar os dados pretendidos. Ora, o regime traçado para um método dito aberto será menos garantístico do que aquele de um método oculto, uma vez que não tem de se acautelar o facto de o visado não ter qualquer tipo de conhecimento acerca da diligência e controlo sobre a mesma. Portanto, por um lado, o regime do artigo 15.º LCC não foi desenhado pensando que seria aplicável a um método oculto de obtenção de prova, e, inversamente, não é adequado subsumir o *malware* ao mesmo por inadequação do regime.

---

[246] RUI COSTA PEREIRA, "A pesquisa…", cit., p. 593
[247] *Ibidem*
[248] PAULO DE SOUSA MENDES, "A privacidade digital posta à prova no processo penal" in *Revista Internacional sobre Razonamiento Probatorio*, n.º 2, 2021, p. 232, disponível em: https://dugi-doc.udg.edu/bitstream/handle/10256/19278/11ArticlesPags225-250.pdf?sequence=1&isAllowed=y (consultado a 19/9/2022)
[249] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 343
[250] *Ibidem*, pp. 276 e 277
[251] RUI COSTA PEREIRA, "A pesquisa…", cit., p. 579
[252] *Ibidem*, p. 580

Por essa razão, acaba por ser inevitável o juízo de inconstitucionalidade a que chega PAULO PINTO DE ALBUQUERQUE, uma vez que «esta intrusão na privacidade da pessoa visada é manifestamente desproporcional, em face do artigo 26.º, n.º1 e 2 e 32.º, nº4 da CRP, que reservam ao juiz os atos instrutórios que representem uma intrusão na privacidade.»[253].

De resto, sempre podemos recorrer à experiência espanhola e alemã, que nos mostram que a utilização de técnicas intrusivas por via de um *software* e a mera pesquisa no âmbito de sistemas informáticos obedecem a um regime diferenciado, por se referirem a realidades distintas. Em bom rigor, entendemos que o regime previsto no artigo 15.º LCC mais se aproxima do regime do artigo 588 *sexies* LECrim (*Registro de dispositivos de almacenamiento masivo de información*) ou da secção §110 StPO (*Durchsicht von Papieren und elektronischen Speichermedien*), os quais regulam o acesso a dados informáticos. Nos referidos diplomas, tal regulação é feita sem prejuízo de, como vimos, se regular simultaneamente, noutros preceitos, a infiltração oculta em sistemas informáticos através da instalação sub-reptícia de um *software*.

Desta feita, defendemos que o regime do artigo 15.º LCC não está desenhado para abarcar a infiltração oculta num sistema informático, por via do recurso a técnicas de *malware*. Em bom rigor, entendemos até que nem sequer terá sido essa a intenção do legislador[254]. Ademais, cumpre igualmente realçar que as razões que nos levam a admitir a compatibilidade e admissibilidade constitucional da utilização do *malware*, expostas em capítulo anterior, não são aquelas que terão levado à introdução deste preceito na nossa ordem jurídica, e por essa razão também não nos parece possível reconduzir estas técnicas ao artigo sob apreço. Na verdade, entendemos que a necessidade de recurso a técnicas como o *malware*, por parte das autoridades de investigação, se prende com a insuficiência

---

[253] PAULO PINTO DE ALBUQUERQUE, *Comentário ao Código de Processo Penal*…, cit., p. 502

[254] Conforme resulta do Diário da Assembleia da República, I-Série, n.º 102, julho de 2009, p. 40, acessível em https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684d5a576376524546535353394551564a4a51584a7864576c326279383077716f6c4d6a42545a584e7a77364e764a5449775447566e61584e7359585270646d4576524546535354457 74d6935775a47593d&fich=DARI102.pdf&Inline=true (consultado a 1/5/2023), em sede de audição parlamentar foi questionada pelo deputado Fernando Negrão a razão pela qual não tinha sido introduzida na proposta de lei do Governo sobre o cibercrime a possibilidade de recurso ao «cavalo de Tróia informático». Donde, e perante a ausência de resposta, não podemos senão concluir, por via do elemento teleológico da interpretação, que tal não terá sido a intenção do legislador.

dos meios legalmente à disposição do das autoridades, de entre os quais a pesquisa de dados informáticos do artigo 15.º LCC.

Assim, e salvo melhor opinião, entendemos que não se poderá reconduzir a utilização de *malware* ao artigo 15.º da LCC, uma vez que, por um lado, nada na letra da lei nos dá essa indicação, até pelo contrário; e, por outro lado, mesmo que chegássemos a tal conclusão através de um esforço interpretativo, seria inevitável um juízo de inconstitucionalidade, por o regime previsto neste preceito não se adequar ao grau de danosidade comportado pela utilização deste tipo de técnicas.

3.2. SOLUÇÕES INTERMÉDIAS

3.2.1. O ARTIGO 15.º, Nº5 DA LCC

Este artigo permite o acesso remoto a sistemas informáticos que sejam acessíveis a partir do sistema que seja alvo de pesquisas nos termos do artigo 15.º, nº1 LCC. Prevendo este preceito um acesso remoto, à semelhança do que sucede no caso de utilização de *malware*, poder-se-ia colocar a questão de saber se este número oferece base legal à mesma[255]. Trata-se, porém, da mera consagração de uma extensão da pesquisa no sistema informático inicial a um outro legitimamente acessível através daquele, em nada diferindo, no que concerne ao recurso ao *malware*, do que foi anteriormente exposto relativamente ao artigo 15.º, nº1, não justificando o facto de os dados se encontrarem armazenados num outro sistema um tratamento diferente. Trata-se, de igual forma, de dados específicos e determinados, armazenados num sistema, aos quais se acede através do sistema inicialmente pesquisado, e do mesmo modo (de forma não oculta), sendo apenas necessária uma extensão da autorização inicial da diligência, sendo que, para todos os efeitos, nada impede que tal permissão de extensão da diligência conste desde logo do mandado inicial[256].

3.2.2. O ARTIGO 19.º, Nº2 DA LCC

Numa perspetiva distinta, DAVID SILVA RAMALHO[257] e JOÃO CONDE CORREIA[258] baseiam a admissibilidade legal da utilização de *malware* como método de obtenção de prova na previsão do nº2 do artigo 19.º LCC. Esta norma dispõe que «sendo necessário o

[255] TIAGO CAIADO MILHEIRO, "Buscas online"…, cit., p. 558; DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 276; JOÃO CONDE CORREIA, "Prova Digital…", cit., p. 42
[256] RUI PEREIRA, "A pesquisa…", cit., p. 576
[257] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 343
[258] JOÃO CONDE CORREIA, "Prova Digital…", cit., p. 43

recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações.». Ora, trata-se de uma formulação extremamente vaga, inserida num artigo que regula as ações encobertas no meio digital, sendo que esta figura está restringida à investigação e prevenção de determinados crimes, e sujeita ao regime da Lei nº101/2001[259].

Um dos argumentos avançados por DAVID SILVA RAMALHO prende-se com a formulação literal do preceito, no sentido de que os «meios e dispositivos informáticos» referidos na norma não se subsumem a qualquer outro dos métodos de prova previstos na legislação portuguesa[260], pelo que terá de se referir a outros meios de prova, uma vez que «entendimento diverso implicaria que o legislador tivesse introduzido nesta norma uma previsão redundante e supérflua que visasse tão-somente permitir ao agente encoberto recorrer a quaisquer outros meios e dispositivos informáticos previstos na lei processual penal (…) o que é afastado pela própria letra da norma que remete o intérprete, naquilo que for aplicável, para o regime da interceção de comunicações.»[261], concluindo que, por isso, se tratará da previsão legal do *malware* como método de obtenção de prova. Com o devido respeito e salvo melhor opinião, entendemos que este argumento não é procedente.

Desde logo, o que parece o autor fazer é proceder à densificação deste conceito de tal modo que viola o princípio da legalidade. Em bom rigor, significativa parte do argumento deste autor baseia-se na densificação do conceito de «meios e dispositivos informáticos», o qual, efetivamente, pode abarcar inúmeras realidades. Porém, tal não é suficiente, à luz do regime vigente, para sustentar a utilização de técnicas de *malware*, uma vez que se trata de um conceito vago. O permanente e inultrapassável conflito entre as exigências comunitárias e a liberdade de realização pessoal[262], e a necessidade de conjugação desses interesses obedece ao princípio da legalidade, carecendo de «uma

[259] Não cumpre no presente estudo proceder a uma análise do regime da Lei nº101/2001, para o qual remete o artigo 19.º, nº1 LCC. Ao que aqui importa, as ações encobertas no meio digital poderão, no que concerne ao agente encoberto, «consistir no "patrulhamento" de sítios da Internet, *chats* ou *newsgroups* abertos ou acedidos com consentimento de um dos participantes, de restes P2P e outas "zonas de risco" do mundo virtual.». Quanto ao agente infiltrado, a sua conduta «consistirá em frequentar o mundo virtual, utilizando uma identidade fictícia, ganhando a confiança dos visados, mantendo-se a par dos acontecimentos e acompanhando a execução dos factos, interagindo com outros participantes em *chats*, *websites*, *blogs* ou fóruns (livremente acessíveis ou de acesso reservado) e praticando atos preparatórios ou mesmo de execução (caso tal se mostre necessário), mas sem determinar ninguém à prática de infrações». Cfr. DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova*…, cit., p. 197 e 199

[260] DAVID SILVA RAMALHO, *Métodos ocultos…*, cit., p. 344

[261] *Ibidem*, p. 345

[262] MARIA DE FÁTIMA MATA-MOUROS, *Juiz das liberdades – desconstrução de um mito do processo penal*, Coimbra, Almedina, 2011, p. 245

estrita e minuciosa regulamentação legal de qualquer indispensável intromissão (…) na esfera dos direitos do cidadão»[263]. Nestes termos, uma lei restritiva «tem de apresentar uma densidade suficiente, isto é, um certo grau de determinação do seu conteúdo, pelo menos no essencial (…)»[264]. Este tipo de exigências não se coaduna, assim, com a vaguidade[265] das normas, sob pena de nos encontrarmos perante «normas processuais penais em branco»[266], marcadas «pela plasticidade e abertas à subsunção dos novos meios tecnológicos de invasão e devassa»[267]. A ausência de densificação legislativa relativamente às realidades inseridas nos «meios e dispositivos informáticos» a que se refere o n.º2 do artigo 19.º LCC não pode, assim, e salvo melhor opinião, dar espaço à subsunção de técnicas tão drasticamente invasivas como é o *malware*.

Para reforçar o argumento de que a norma do artigo 19.º, nº2 se refere ao *malware*[268], o autor acrescenta ainda, quase legitimando a subsunção daquelas técnicas a esse conceito, que terão de se tratar de técnicas que operem de modo materialmente semelhante à figura do agente encoberto[269]. O autor utiliza o regime desenhado para uma determinada figura, com características materialmente idênticas às do *malware*, para sustentar uma interpretação deste tipo. Entendemos que o autor se socorre de uma lógica invertida, na medida em que, ao invés de propor um regime adequado às especificidades do *malware,* tenta submeter este tipo de técnicas àquele que parece ser o regime existente mais adequado. Em vez de concluir pela inexistência de regime na lei processual penal portuguesa, o autor parece optar por "forçar" a inserção de uma realidade no regime legal à custa dos princípios constitucionais, tendo em conta que nos encontramos perante um tipo de técnicas que carecem de ser expressa e cuidadosamente reguladas, sob pena de inconstitucionalidade. Na verdade, nem o próprio autor escapa à conclusão de

[263] JORGE DE FIGUEIREDO DIAS, *Direito Processual Penal…,* cit., pp. 74-75
[264] JOSÉ CARLOS VIEIRA DE ANDRADE, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, Coimbra, Almedina, 6ª edição, 2021, pp. 287-288
[265] Segundo MARIA LUÍSA DUARTE, "A discricionariedade administrativa e os conceitos jurídicos indeterminados (contributo para uma análise da extensão do princípio da legalidade)", in *Boletim do Ministério da Justiça*, nº370, 1987, p. 52, vaguidade será um tipo de indeterminabilidade do conceito que «(…) permite uma informação de extensão longa, mas compreensão escassa, apresentando uma orla conceptual (ou zona de dúvida) muito ampla (…)», sendo que, em nosso entender, a expressão «meios e dispositivos informáticos» engloba um conceito vago naquela aceção.
[266] MARIA DE FÁTIMA MATA-MOUROS, *Juiz das liberdades…,* cit., pp. 247-248
[267] MANUEL DA COSTA ANDRADE, "*Bruscamente no Verão Passado…*", cit., p. 113
[268] DAVID SILVA RAMALHO, *Métodos Ocultos…,* cit., p. 346
[269] *Ibidem*

inconstitucionalidade daquele que diz ser o regime existente para a utilização de *malware*[270], como veremos adiante.

Nesta senda, parece ainda DAVID SILVA RAMALHO basear-se no facto de os meios e dispositivos informáticos referidos no artigo 19.º, n.º2 LCC estarem, por força da sua inserção sistemática, limitados ao contexto excecional das ações encobertas[271], e por isso terem de ser meios com caráter insidioso e invasivo, para concluir que se tratará da consagração de *malware*. Em nosso entendimento, este caráter excecional levaria a que, eventualmente, se acautelasse o nível de invasividade comportado por estas técnicas, o que poderia constituir, para alguns, um argumento que sopesasse a ausência de consagração legal expressa, aligeirando a gravidade da situação. Contudo, continuamos a discordar deste entendimento. Por um lado, o artigo 19.º, n.º2 pode ser interpretado no sentido de autorizar a cumulação das ações encobertas com outros métodos de obtenção de prova (desenvolveremos este ponto infra). Por outro lado, o argumento de que se encontram circunscritos ao contexto das ações encobertas, e apenas quando os demais métodos ocultos sejam incapazes de dar resposta às exigências de investigação, tratando-se de um meio duplamente excecional[272] permanece insuficiente, porque ao depender da consagração de *malware* nesse artigo, não pode servir de base à sustentação do argumento de que o *malware* se encontra previsto nesse mesmo artigo.

Efetivamente, a utilização de *malware* como método de investigação, a ser consagrada, terá de ter em consideração o caráter oculto, insidioso e atentatório de direitos fundamentais deste tipo de programas. Donde, deverá ter um caráter excecional e ser estipulado com requisitos materiais e formais que permitam o controlo da sua utilização, assegurando que é respeitado o seu caráter excecional. Não obstante, parece-nos que vai demasiado longe o argumento de que, se se trata de meios e dispositivos informáticos necessários no âmbito das ações encobertas, quase como última *ratio,* então trata-se, quase indubitavelmente, da consagração do *malware*.

Ademais, ainda que existisse margem para uma interpretação como a que propugna este autor, o facto de o legislador ter optado por se referir a «meios e dispositivos informáticos» e ter remetido para o regime da interceção de comunicações não impede que se esteja a referir a outras realidades que não a admissibilidade de

[270] DAVID SILVA RAMALHO, *Métodos Ocultos…,* cit., pp. 351 e ss.
[271] *Ibidem*, p. 345
[272] Por apenas ser admissível, subsidiariamente, em contexto de ações encobertas.

utilização de *malware*. Em bom rigor, poderá estar em causa a cópia de dados obtidos nos *chats* em que o agente se encontra, o que pode nada ter que ver com a utilização de *malware*[273]. Donde, parece-nos que afirmar que «uma norma que, logicamente, ao não se limitar a invocar outros meios de obtenção de prova típicos, terá surgido para colmatar a insuficiência dos demais meios processuais existentes para abrangerem estes meios e dispositivos informáticos (…)»[274] constitui um salto incompreensível no raciocínio que leva à conclusão de que o legislador não terá tido qualquer outra intenção além de consagrar a utilização de técnicas como o *hacking* e o *malware*[275]. O legislador terá antes pretendido consagrar a possibilidade de cumulação das ações encobertas em meio digital com outros métodos de obtenção de prova[276].

Por último, a conclusão de que a consagração legal da utilização do *malware* como método de obtenção de prova se encontra plasmada no nº2 do artigo 19.º LCC não deixa de colocar questões de constitucionalidade, semelhantes às suscitadas anteriormente a propósito do artigo 15.º LCC. Efetivamente, DAVID SILVA RAMALHO chama à colação os problemas suscitados por esta solução[277], salientando que tal regime é «manifestamente inadequado para regular aquele que (…) será o meio de obtenção de prova mais invasivo e intensamente restritivo de direitos fundamentais consagrado na lei processual penal portuguesa»[278]. Desde logo, o preceito sob análise não apresenta uma regulação clara, precisa e previsível dos pressupostos e condições da admissibilidade de utilização do *malware*, em violação dos artigos 18.º, nº2 e 26.º, nº2 da CRP[279]. Ademais, suscita também questões de proporcionalidade, tendo em conta o catálogo de crimes previsto no regime das ações encobertas, considerando que a utilização de *malware* deveria estar sujeita a um catálogo mais restrito[280]. Por outro lado, o autor suscita a questão da duração temporal deste método de obtenção de prova, defendendo que o mesmo não poderia ser igual ao das escutas (três meses)[281]. Por último, o autor critica ainda o facto de não ter

[273] DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova*…, cit., p. 204
[274] DAVID SILVA RAMALHO, *Métodos ocultos…*, cit., p. 345
[275] *Ibidem*, p. 346
[276] DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova*…, cit., p. 209
[277] DAVID SILVA RAMALHO, *Métodos ocultos…*, cit., p. 351
[278] *Ibidem*
[279] *Ibidem*, pp. 351 e ss.
[280] *Ibidem*, p. 351
[281] *Ibidem*, p. 352

sido previsto um relatório técnico da utilização deste método de prova, o que permitiria a sindicância da utilização do mesmo[282].

3.3. SOLUÇÃO RESTRITA: AUSÊNCIA DE CONSAGRAÇÃO LEGAL

Por tudo isto, entendemos que, salvo melhor opinião, e numa formulação algo redundante, o facto de não haver uma regulação expressa da utilização do *malware* será em si um indício de que não se encontra consagrado na lei. Efetivamente, não só estas técnicas não se encontram expressamente previstas, como, na verdade, chegar lá por meio de um esforço de interpretação de outros preceitos sempre colocaria questões de inconstitucionalidade, o que torna difícil defender a sua admissibilidade[283]. Ou seja, o que parece estar em causa é: ou não se encontra regulado porque efetivamente não há qualquer preceito que o faça expressamente e por isso trata-se de um método ilegal e proibido de obtenção de prova (artigo 126.º, nº3 CPP); ou se desencanta, através de um tremendo esforço de argumentação, um preceito legal na previsão do qual se tenta inserir este método de prova para concluir que o mesmo é inconstitucional. Afigura-se-nos inadequado concluir pela consagração legal deste tipo de técnicas, e não aderimos a nenhuma das perspetivas apresentadas, propendendo para o entendimento mais restrito da doutrina maioritária[284].

Neste sentido, a maioria dos autores rejeita a admissibilidade da utilização de *malware* (mesmo que se refiram às buscas *online*) em virtude da ausência de previsão legal expressa, sendo igualmente esta a orientação que tendemos a seguir. Evidentemente, não olvidamos a necessidade da utilização de *malware* na investigação criminal contemporânea, pois não é possível ignorar as valias trazidas por este método. Pelo contrário, no capítulo 2.1. e 2.2. tentámos evidenciar as razões que justificam a utilização deste tipo de técnicas, e dentro de que moldes pensamos que tal poderá ser regulado no nosso ordenamento jurídico. Certo e indiscutível é, contudo, que tal utilização jamais se

[282] DAVID SILVA RAMALHO, *Métodos ocultos…*, cit., p. 352

[283] Sem prejuízo de se tratar de interpretações que, até ao momento, não foram fiscalizadas pelo Tribunal Constitucional

[284] JULIANA SOUSA CAMPOS, *O malware…,* cit., pp. 101 e 102; DANIEL BENTO ALVES, "Uso de *malware…",* cit., pp. 28 e ss.; MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…"* cit., pp. 165-169; BENJAMIM SILVA RODRIGUES, *Da Prova Penal…,* cit., pp. 379 e 380; SÓNIA FIDALGO, "A utilização de inteligência artificial…", cit., p. 153; RITA CASTANHEIRA NEVES, *As ingerências nas comunicações…,* cit., p. 196; ARMANDO DIAS RAMOS, *O Agente Encoberto*…, cit., p. 280

poderá fazer em atropelo dos princípios constitucionais vigentes, nomeadamente, princípio da reserva de lei[285].

3.4. ATIPICIDADE DA UTILIZAÇÃO DE *MALWARE*: CONSEQUÊNCIAS

Aqui chegados, pretendemos abordar sucintamente as consequências da ausência de previsão legal que habilite as autoridades a recorrer a técnicas de *malware* em sede de investigação criminal e recolha de prova. Ou seja, abordar que questões se suscitam perante a constatação de que o *malware* é, à luz da legislação vigente, um método atípico de obtenção de prova, com aptidão para comprimir drasticamente diversos direitos fundamentais.

No primeiro capítulo do presente trabalho concluímos categoricamente pela inadmissibilidade de métodos de obtenção de prova ocultos atípicos, em virtude da sua propensão para transgredirem o conteúdo essencial de direitos fundamentais[286], pois que apenas serão legítimos se a respetiva admissibilidade estiver coberta por uma previsão legal. Preferencialmente, uma norma que regule de forma suficiente as condições e requisitos de admissibilidade de utilização, de tal modo que se considere cumprido o princípio da proporcionalidade. Sendo a infiltração sub-reptícia num sistema informático através da instalação de um qualquer *software* um método oculto, com as consequências para os direitos fundamentais já anteriormente analisadas, não podemos deixar senão de concluir que, à luz do quadro legal vigente, o recurso a este tipo de técnicas constitui um método proibido de prova, nos termos do artigo 126.º, n.º3 CPP.

Não fosse o tema já premente em virtude de se tratar de uma prática difundida na investigação criminal de vários outros países, também no nosso ordenamento jurídico começam a soar os sinos de utilização deste tipo de técnicas[287], transpondo-se assim o problema da teoria para a prática.

A atipicidade da utilização de técnicas de *malware* no processo penal português e a sua consequente proibição, nos termos dos artigos 126.º, nº3 CPP e 32.º, nº8 CRP,

---

[285] DANIEL BENTO ALVES, "Uso de *malware* …"; cit., p. 29; MANUEL DA COSTA ANDRADE, "Métodos ocultos…", cit., p. 540

[286] JOÃO GOUVEIA CAIRES, "Métodos ocultos na criminalidade económico-financeira…", cit., p. 72

[287] Recentemente, no caso mediático conhecido como *Football Leaks*, o advogado do arguido suscitou a inadmissibilidade de alguma prova por considerar que as autoridades tiveram acesso remoto ao computador através de técnicas de phishing. Cfr. INÊS BANHA "Football Leaks – PJ usou "prova proibida" para chegar a Rui Pinto, acusa advogado", in *Jornal de Notícias*, 6 de janeiro de 2023, disponível em: https://www.jn.pt/justica/pj-usou-prova-proibida-para-chegar-a-rui-pinto-acusa-advogado-15610844.html (consultado em 2/5/2023)

obriga-nos a confrontar uma realidade do processo penal, que choca, *a priori*, a maioria dos cidadãos: a ineficácia no combate à criminalidade mais grave, o qual é limitado pelo regime das proibições de prova que impõe o respeito pelos direitos fundamentais. No entanto, o interesse na realização efetiva da justiça penal também exige salvaguarda[288], a qual indiscutivelmente passa pelo sacrifício desses direitos fundamentais. A tecnologia avança, surgem novos meios de cometimento de crimes e de obstaculizar a sua investigação. Do mesmo modo, surgem novos meios técnicos de investigação. No entanto, nas palavras de COSTA ANDRADE, «o que é tecnicamente possível, não é, só por si e sem mais, legítimo»[289], donde «o recurso a um novo meio técnico (oculto e invasivo) de investigação em processo penal (…) só é possível depois de prévia – explícita e autónoma – legitimação legal»[290]. Assim, o que não se compreende é a inércia do legislador nesta matéria.

Conforme explicitámos, a consagração de *malware* como método de investigação não contende de forma inadmissível com o núcleo essencial dos direitos fundamentais. Isto é, entendemos que a CRP oferece abertura suficiente para a consagração, pelo legislador ordinário, deste tipo de técnicas no âmbito do processo penal, e mediante a previsão de determinados requisitos (p.e., autorização judicial, catálogo de crimes, catálogo de sujeitos, limite temporal), em cumprimento do princípio da proporcionalidade. Em bom rigor, o fundamento axiológico do regime das proibições de prova, segundo o qual existem limites intransponíveis à prossecução da verdade no processo penal[291], não podendo o sistema superar os seus problemas à custa do desrespeito do valor autónomo da pessoa[292], não implica que todos os direitos fundamentais sejam incomprimíveis, como de resto se tem vindo a explicitar ao longo do presente texto.

A própria CRP, no artigo 32.º, n.º8 e o CPP, no artigo 126.º, nº3, exprimem a possibilidade de obtenção de prova com limitação dos direitos aí referidos, dentro dos limites da lei. Como vimos, tal terá de ser feito nos termos do artigo 18.º, n.º2 CRP, por se tratar da restrição, por via legal, de direitos fundamentais. Assim, não deixando de estar perante uma proibição de prova em virtude de o recurso a técnicas de *malware* não se

[288] MANUEL DA COSTA ANDRADE, *Sobre as proibições de prova…,* cit., p. 33
[289] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…",* cit., p. 150
[290] *Ibidem*, p. 113
[291] *Ibidem*, p. 123
[292] *Ibidem*, p. 124

encontrar legalmente previsto (donde, não entra na salvaguarda dos artigos 126.º, n.º3 CPP e 32.º, nº8 CRP), e não sendo a nulidade daí decorrente de menor significado do que aquela decorrente das proibições absolutas de prova[293], somos levados à constatação de que, no estádio atual do estudo jurídico sobre esta problemática, e perante os obstáculos colocados à investigação criminal, trata-se de uma proibição incompreensível.

Melhor dizendo, é incompreensível, atenta a consequência inultrapassável da proibição de prova, que o nosso regime jurídico não se encontre, ainda, adaptado à realidade atual, em face das carências que se fazem sentir. Entendemos que se trata de uma necessidade premente para a investigação criminal, o que é evidenciado pelas medidas adotadas noutros ordenamentos jurídicos, e até a nível internacional[294]. Em bom rigor, a proibição de produção de prova com que nos confrontamos decorre somente da ausência de norma habilitante que legitime este tipo de medidas, e entendemos que não se trata de uma "lacuna" intencional. Isto é, o legislador não terá procedido à ponderação dos interesses em jogo e optado pela não consagração deste tipo de técnicas. Pelo contrário, entendemos que se trata de inércia na adaptação do regime legal às novas possibilidades técnicas. Caso o legislador venha a intervir nesta matéria, tratar-se-á apenas, em nosso entender, de dotar as autoridades de investigação criminal dos meios necessários para uma investigação eficaz. Até lá, há que chamar a atenção para o risco que se corre de este tipo de técnicas serem utilizadas à margem da legalidade[295], o que de resto ficou evidenciado que pode suceder com o exemplo da utilização de GPS. Assim, urge realçar novamente que é da maior premência que o legislador tome uma atitude no âmbito desta matéria.

[293] PAULO DE SOUSA MENDES, "As proibições de prova…"; cit., p. 148
[294] *Vide*, p. 14 do presente texto
[295] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…",* cit.,

4. CONTRIBUTOS PARA ALTERAÇÃO DA ABORDAGEM DO PROBLEMA

Aqui chegados, percebemos que o problema sob análise não é de somenos, e ainda que a jurisprudência acerca do tema seja escassa, senão mesmo inexistente[296], já se assiste à sua discussão no seio da doutrina. Não obstante, das várias obras que pudemos consultar constatámos, que, no âmbito da nossa doutrina, a problemática é suscitada de duas perspetivas distintas. Por um lado, encontramos os autores que se referem ao *malware* como método de obtenção de prova, encarando-o quase como uma realidade unitária e indistinta, apesar do reconhecimento da sua complexidade[297]. Por outro lado, e como evidenciámos a propósito da escolha da terminologia adotada, outros autores referem-se às "buscas *online*" e à "vigilância na fonte"[298], enquanto realidades distintas (que são), mas pressupondo, em ambos os casos, a utilização de técnicas de *malware* para proceder a esse tipo de diligências.

Assim, não só percebemos que não é completamente irrelevante a escolha do termo a utilizar na análise desta problemática[299], como igualmente se constata que o estádio atual de tratamento da mesma no seio da nossa doutrina carece de uma abordagem diferente, que tome em consideração o facto de, ao falarmos de *malware* no âmbito do processo penal, nos referimos a um *modo de execução* de certas diligências, ao passo que quando nos referimos às buscas *online*, à vigilância na fonte das telecomunicações e até às ações encobertas, nos referimos a diligências autónomas, as quais, contudo, podem recorrer a técnicas de *malware*.

Isto é, entender o *malware* como um método de prova em si e como um todo é inadequado e falacioso. Em bom rigor, não se toma em consideração a complexidade deste tipo de técnicas e desconsidera-se, no limite, as diferentes realidades que podem ser abarcadas, e assim, ignora-se os diferentes graus de lesão dos diferentes direitos comportados por este tipo de técnicas[300]. Ademais, *malware,* por si, significa apenas

---

[296] Das poucas decisões jurisprudenciais nas quais a questão acerca da infiltração oculta através de um *software* se colocou, nenhuma abordou o problema central, surgindo esta questão residualmente.
[297] DAVID SILVA RAMALHO, *Métodos ocultos…,* cit.,; JULIANA SOUSA CAMPOS, *O Malware…,* cit.,; DANIEL BENTO ALVES, "Uso de *malware…",* cit.; SÓNIA FIDALGO, "A utilização de inteligência artificial…", cit.
[298] Referindo-se apenas às buscas *online* com recurso aos denominados cavalos de Tróia, cfr. PAULO PINTO DE ALBUQUERQUE, *Comentário ao Código de Processo Penal…*, cit., p. 502; DUARTE RODRIGUES NUNES *O problema da admissibilidade…,* cit., p. 812. Referindo-se, em circunstâncias diversas, às buscas *online* e à vigilância na fonte das telecomunicações, cfr. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado…"*, cit., pp. 165-166; BENJAMIM SILVA RODRIGUES, *Da Prova Penal…,* cit., pp. 376 e ss. e 470 e ss. Referindo-se à vigilância na fonte, cfr. ARMANDO DIAS RAMOS, *O Agente Encoberto…,* cit., p. 19
[299] Daí que, ao longo do presente estudo, tenhamos preferencialmente utilizado a expressão «técnicas de malware».
[300] Por exemplo, refere DAVID SILVA RAMALHO que não está em causa a intromissão nas telecomunicações.

«*malicious software»,* dependendo o seu significado na prática daquilo para o que for programado em cada caso. Por isso, tentar reconduzir este tipo de técnicas à previsão de um determinado preceito legal parece-nos redutor do impacto que estas podem ter na investigação criminal. Ainda que nos casos analisados supra[301] se tratasse da simples subsunção de algum dos tipos destas técnicas a um preceito, entendemos que, em virtude de se tratar de técnicas que permitem diferentes possibilidades, a abordagem do problema não deverá passar por tentar reconduzi-las a um determinado preceito legal[302]. Em nossa opinião, como evidenciámos anteriormente, não há na lei processual penal portuguesa qualquer norma que legitime o uso destas técnicas, e entendemos que as mesmas, a virem a ser expressamente reguladas, também não têm de estar sujeitas a um regime unitário consagrado num determinado preceito legal.

Por outro lado, distinguir absolutamente as "vigilâncias na fonte" das "buscas *online*", ignorando que para ambas são utilizadas técnicas da mesma natureza (oculta e invasiva) também não nos parece adequado. Ou seja, apesar de os autores que adotam esta abordagem tomarem em consideração que, naqueles casos, estão em causa realidades distintas, em função dos direitos comprimidos e respetivo grau de lesão, parecem desconsiderar que, ainda assim, a técnica utilizada para ambas é a mesma, e, desse modo, tem características que as aproximam[303].

Assim, a nosso ver, o mais adequado será propugnar por uma abordagem que conjugue estas duas perspetivas, no sentido de reconhecer que as técnicas de *malware* apresentarão todas um grau de danosidade mínimo comum, o que se deve repercutir no respetivo regime legal. No entanto, dependendo do desiderato pretendido e da diligência no âmbito da qual são utilizadas, poderão ter um tratamento distinto, o que, de resto, decorre, a nosso ver, do princípio da proporcionalidade. Na verdade, entendemos que, perante uma visão da problemática como a que pretendemos propor, até em termos sistemáticos seria mais aconselhável a introdução deste tipo de técnicas no âmbito de artigos ou diligências já previstas na lei. Vejamos.

---

[301] *Vide*, capítulo 3

[302] Indo um pouco mais além na sua análise, em virtude do reconhecimento da complexidade deste tipo de programas, cfr. DUARTE RODRIGUES NUNES, *O problema da admissibilidade…,* cit., pp. 809 e ss.

[303] Nomeadamente, sempre em causa estará a afetação do direito à integridade e confidencialidade dos sistemas informáticos, como um todo, em virtude da instalação de um programa no dispositivo visado.

Consabidamente, os artigos 15.º, 18.º e 19.º LCC[304] regulam realidades diferentes, pelo que igualmente consagram regimes jurídicos diferentes. Em bom rigor, técnicas de *malware* podem ser utilizadas no âmbito de qualquer um daqueles regimes. Por exemplo, GONÇALO GAGO DA CÂMARA[305] avança uma proposta de consagração de um regime de vigilância e captura oculta de dados, o qual, recorrendo a técnicas de infiltração oculta em sistemas informáticos através de um *software*, mais se aproximará, de resto, do regime das pesquisas informáticas do artigo 15.º LCC. Na verdade, pode até pretender-se consagrar a mera pesquisa de dados informáticos específicos e determinados, mas oculta, por via da instalação de um *software* no sistema do visado. Por outro lado, poucas dúvidas surgirão ao afirmar-se que a vigilância na fonte das telecomunicações se aproxima, necessariamente, do regime da interceção em comunicações. Por último, há quem defenda a utilização de *malware* no âmbito das ações encobertas digitais, e a prática de investigação criminal mostra até que se encara as ações encobertas como a instalação de *software* num dispositivo informático procedendo à monitorização total de toda a atividade desenvolvida nesse sistema[306], ao ponto de não ser sequer necessário um agente físico encoberto no sistema.

Com isto, pretendemos colocar em evidência como este tipo de técnicas podem estar ao serviço da investigação criminal das mais variadas formas, o que comprova a desadequação de um regime único para a sua utilização em processo penal. Na verdade, a experiência espanhola demonstra o quão complicado se pode tornar, para o intérprete, a consagração da utilização de *malware* no âmbito dos *registros remotos de equipos informáticos*, sem se operar uma referência à interceção de comunicações, o que instalou na doutrina espanhola o debate sobre a conjugação desse preceito com aquele que prevê a interceção de comunicações[307]. Pelo contrário, a experiência alemã evidencia a adequação do estabelecimento de um regime que preveja a utilização de técnicas de *malware* no âmbito de diferentes diligências[308].

---

[304] Referimos estes artigos por se tratarem dos regimes mais comummente invocados na tentativa de encontrar uma base legal para a utilização de *malware* ou como regimes aplicáveis a esta realidade, sem prejuízo de se poder proceder à utilização destas técnicas no âmbito de outros regimes.
[305] GONÇALO GAGO DA CÂMARA, "A captura ou monitorização encoberta online de dados informáticos em processo penal: uma contribuição acerca da sua admissibilidade no ordenamento jurídico português", Dissertação de Mestrado, p. 74, disponível em: https://repositorio.ul.pt/bitstream/10451/55027/1/ulfd0150682_tese.pdf (consultado a 8/5/2023)
[306] ARMANDO DIAS RAMOS, *O Agente Encoberto…,* cit., p. 20
[307] *Vide*, capítulo 2.3.2.
[308] *Vide*, capítulo 2.3.3.

Assim, consideramos que seria não só possível, como aconselhável, adaptar o regime jurídico à realidade atual, através da possibilitação de recurso a técnicas de *malware* no âmbito da investigação criminal, no seio de diferentes diligências. Fulcral, é, sim, a necessidade de consagração legal expressa e suficiente deste tipo de técnicas, sob pena de as mesmas serem inadmissíveis, e constituírem prova proibida. Efetivamente, ao afirmar que a vigilância na fonte das telecomunicações através da utilização de *malware* comprime necessariamente o direito ao sigilo sobre as telecomunicações, e legitimando a norma do artigo 18.º LCC uma intromissão nas telecomunicações por parte das autoridades de investigação criminal, facto é que aquela não se encontra legitimada por esta[309], porque, como vimos, não se trata da "mera" intromissão nas telecomunicações[310].

Deste modo, a introdução do uso de técnicas de *malware* no âmbito do processo penal português carecerá de um regime suficientemente adequado à proteção dos direitos fundamentais, *maxime*, da privacidade, porque sempre estará em causa o desenvolvimento de um *software* a ser instalado sub-repticiamente. Não obstante, a programação concreta do *software* a utilizar dependerá da finalidade que se pretenda atingir com a sua utilização, e perante a panóplia de possibilidades admitidas neste seio, entendemos que, sistematicamente, seria mais adequado a admissibilidade de utilização de um *software* oculto em vários preceitos, em função das finalidades concretamente prosseguidas pela investigação. Ademais, o respetivo regime, ainda que deva obedecer a requisitos mínimos de salvaguarda dos direitos fundamentais, poderá não ter os mesmos limites e condicionalismos, pois os direitos afetados não o serão todos no mesmo grau.

Queremos com tudo isto dizer que defendemos a indiscutível necessidade deste tipo de técnicas no âmbito da investigação criminal, não obstante, tal terá de passar pela consagração de um regime adequado, o que entendemos implicar a adaptação de regimes já existentes às novas realidades. Nas palavras de ARMANDO DIAS RAMOS, «constata-se que urge definir novas políticas legislativas de obtenção de prova na área das novas tecnologias por estas estarem mais avançadas e ser possível fazer melhor pela investigação criminal utilizando ferramentas disponíveis atualmente, mas que a lei não regula a sua utilização»[311].

---

[309] BENJAMIM SILVA RODRIGUES, Da Prova Penal…, cit., p. 479; DAVID SILVA RAMALHO, *Métodos ocultos…,* cit., p. 342
[310] *Vide*, capítulo 2.2.
[311] ARMANDO DIAS RAMOS, *O Agente Encoberto…,* cit., p. 53

CONCLUSÕES

I. Sendo indiscutível na sociedade atual a necessidade de novos meios de investigação criminal para fazer face aos obstáculos colocados pelo progresso tecnológico, a utilização de técnicas de *malware* no âmbito do processo penal confronta o intérprete com questões complexas.

II. No processo penal, o recurso a *malware* materializa-se na infiltração oculta num sistema informático por via da instalação de um *software*, através da qual se permite a monitorização da atividade desenvolvida nesse sistema informático e a posterior recolha de dados.

III. As tarefas a executar, no caso concreto, dependem das funcionalidades que tenham sido atribuídas ao *malware*, ou seja, depende daquilo para que o *software* tenha sido programado, estando tal definição no poder de quem o desenvolve, em função das necessidades da investigação criminal em concreto. Donde, não é um programa único que funcione de forma linear.

IV. Assim, este tipo de técnicas poderão ser utilizadas para interceção de comunicações, recolha de dados armazenados ou até no âmbito de ações encobertas em ambiente digital.

V. Porém, atendendo ao facto de, através da utilização de *malware*, se poder recolher prova interna (i.e., dados armazenados, não armazenados, e produzidos em tempo real) e prova externa (i.e., ativação de *hardware*, ativando o microfone e/ou a câmara do dispositivo), este tipo de técnicas são suscetíveis de colocar em crise diversos direitos fundamentais, ainda que de modo e em graus distintos.

VI. Este tipo de técnicas poderão configurar uma intrusão no direito à inviolabilidade do domicílio, caso se permita ativação do *hardware* de um dispositivo que se encontre dentro de um domicílio. Assim, a afetação concreta deste direito encontra-se dependente de o regime legal permitir este grau de espionagem, e entendemos que apenas o será em situações residuais.

VII. O direito ao sigilo das telecomunicações pode ser indubitavelmente restringindo pela utilização deste tipo de técnicas, apesar de as mesmas não se encontrarem legitimadas pelas normas vigentes que permitem intromissão nas telecomunicações. Uma das grandes valias do recurso a este tipo de técnicas

na investigação criminal prende-se com a possibilidade de vigilância na fonte das comunicações, interferindo, assim, a utilização de *malware* com a liberdade comunicativa.

VIII. O direito à autodeterminação informativa é igualmente suscetível de ser lesado em virtude da possibilidade de acesso a dados pessoais constantes do dispositivo visado. O direito à integridade e confidencialidade dos sistemas informáticos oferece o maior grau de tutela contra as invasões decorrentes da utilização de *malware*, pois sempre se estará a afetar o sistema informático como um todo.

IX. Configurando todos estes direitos manifestações concretas do direito à privacidade, reclama-se em qualquer caso uma tutela acrescida para proteção da área nuclear da privacidade, em função da concreta funcionalidade do *malware* ativada.

X. Sendo certo que a admissibilidade destas técnicas encontra justificação na sua necessidade para a descoberta da verdade material e realização da justiça, e que os direitos mencionados não são absolutos, o recurso a este tipo de técnicas suscita ainda questões ao nível de outros princípios do processo penal e relativamente ao facto de a compressão dos referidos direitos se poder estender a terceiros.

XI. Tratando-se de um método oculto de obtenção de prova, a possibilidade de compressão daqueles valores fundamentais está sujeita a uma intransponível reserva de lei, sob pena de se tratar de prova proibida, nos termos do artigo 126.º, nº3 CPP. Isto é, a mera constatação da carência deste tipo de tecnologias no processo penal, que justifica a restrição daqueles direitos, aliada à possibilidade técnica de recurso às mesmas, não legitima, por si só, o seu uso em processo penal. Antes, reclama-se a intervenção do legislador para a introdução deste tipo de métodos de investigação, através de lei expressa e suficiente, dando cumprimento às imposições constitucionais.

XII. Constatando que outros Estados já procederam à regulação da utilização de técnicas de infiltração oculta em sistemas informáticos, consagrando requisitos e condições de admissibilidade que acautelam a danosidade deste tipo de técnicas, concluímos que esse não é o caso no nosso ordenamento jurídico.

XIII. Não obstante, no seio da doutrina portuguesa, encontramos divergências quanto à consagração legal, e respetivos termos, da utilização de *malware* no processo penal. Num espetro alargado de entendimentos, há quem subsuma este tipo de técnicas ao artigo 15.º LCC (solução alargada), ao artigo 15.º, nº5 LCC, e 19.º, nº2 LCC (soluções intermédias), e ainda quem propugne pela aplicação do regime do artigo 18.º LCC.

XIV. Aderimos a uma solução restrita, segundo a qual é indefensável, à luz da lei vigente e das imposições constitucionais para a regulação deste tipo de meios de prova, que a lei processual penal portuguesa admita, atualmente, a utilização dos mesmos. Assim, o recurso a este tipo de técnicas contamina a prova obtida, por proibida nos termos do artigo 126.º, nº3 CPP.

XV. Ademais, a abordagem que a maioria da doutrina portuguesa adota no tratamento desta questão ignora a complexidade das técnicas de *malware*, encarando este como um método de prova como um todo em si, sujeitando-o a um regime unitário. Como explicitámos, tal desconsidera a natureza deste tipo de técnicas e obstaculiza o desenvolvimento desta problemática.

XVI. Assim, sendo premente que o legislador consagre a utilização de técnicas de *malware* no âmbito do processo penal português, uma vez que o progresso tecnológico e os meios ao serviço dos delinquentes não voltarão atrás, sendo antes necessário que se adapte a legislação à realidade desta era digital; é aconselhável que se introduza o recurso a este tipo de técnicas em diferentes preceitos, em função do modo e grau de afetação dos direitos fundamentais em concreto, ao invés de submeter estas técnicas a um único preceito.

BIBLIOGRAFIA

ABEL, Wiebke/ SCHAFER, Burkhard, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822" *SCRIPTed – A Journal of Law, Technology and Society*, Volume 6, n.º 1, April 2008, pp.107-123, disponível em http://script-ed.org (consultado a 21/3/2023)

ADAMS, Devin M., "The 2016 amendments to criminal rule 41: national search warrants to seize cyberspace, "particularly" speaking", *University of Richmond Law Review*, vol. 51, 2017, disponível em: https://scholarship.richmond.edu/law-student-publications/146/#:~:text=Rule%2041%2C%20governing%20searches%20and%20seizures%2C%20now%20permits,devices%20in%20multiple%20districts%20anywhere%20in%20the%20country (consultado a 22/3/2023)

ALBERGARIA, Pedro Soares de, "Artigo 125º CPP" in *Comentário Judiciário do Código de Processo Penal*, Tomo II, Coimbra, Almedina, 2019

ALBREHCT, Hans-Jörg, "Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos." in *Que futuro para o direito processual penal?: Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, (coord. Mário Ferreira Monte, et al.), Coimbra, Coimbra Editora, 2009, pp. 725-743

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

ALMEIDA, Carlos Rodrigues de, "O registo de voz e imagem – notas ao artigo 6.º da lei nº5/2002, de 11 de janeiro", in *Revista Portuguesa de Ciência Criminal*, ano 14, nº3, julho-setembro 2004, pp. 369-379

ALVES, Daniel Bento, "Uso de *malware* em investigação criminal" in *Actualidad Jurídica Uría Menéndez*, 2017, pp. 19-30, disponível em: https://www.uria.com/documentos/publicaciones/5655/documento/AJUM-47-001.pdf?id=7642&forceDownload=true (consultado a 19/10/2022)

ANDRADE, José Carlos Vieira de, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, Coimbra, Almedina, 6ª edição, 2021

ANDRADE, Manuel da Costa

- *"Bruscamente no Verão Passado", a reforma do Código de Processo Penal: Observações críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra, Coimbra Editora, 2009

- "Métodos ocultos de investigação, Plädoyer para uma teoria geral", in *Que futuro para o direito processual penal?: Simpósio em Homenagem a Jorge de Figueiredo Dias, por*

ocasião dos 20 anos do Código de Processo Penal Português, (coord. Mário Ferreira Monte, et al.), Coimbra, Coimbra Editora, 2009, pp. 525-551

- "Domicílio, Intimidade e Constituição (anotação crítica do acórdão 364/2006 do Tribunal Constitucional)" in *Revista Brasileira de Ciências Criminais*, ano 21, vol. 100, janeiro-fevereiro de 2013, pp. 55-88

- *Sobre as proibições de prova em processo penal*, 2ª ed., Coimbra, Gestlegal, 2022

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

ASCENSÃO, José de Oliveira, "O Cibercrime", separata de *Direito Penal Económico e Financeiro: conferências do curso pós-graduado de aperfeiçoamento* (coord. Maria Fernanda Palma, et al.), Coimbra, Coimbra Editora, 2012

BRITO, Maria Beatriz, *Novas Tecnologias e Legalidade da Prova em Processo Penal. Natureza e enquadramento do GPS como método de obtenção de prova*, reimpressão, Coimbra, Almedina, 2020

CAIRES, João Gouveia, "Métodos ocultos na criminalidade económico-financeira: entre a (a)tipicidade e a cumulação", in *JULGAR,* nº38, 2019, pp. 45-84 disponível em: http://julgar.pt/wp-content/uploads/2019/05/JULGAR38-04-JC.pdf (consultado a 25/11/2022)

CÂMARA, Gonçalo Gago da, "A captura ou monitorização encoberta online de dados informáticos em processo penal: uma contribuição acerca da sua admissibilidade no ordenamento jurídico português", Dissertação de Mestrado, disponível em: https://repositorio.ul.pt/bitstream/10451/55027/1/ulfd0150682_tese.pdf (consultado a 8/5/2023)

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

CANOTILHO, J.J. Gomes / MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volume I, 4.ª ed., Coimbra, Coimbra Editora, 2007

CARDOSO, Rui, "Apreensão de Correio Eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei 109/2009, de 15.IX", *Cibercriminalidade e Prova Digital*, Coleção Formação Contínua, CEJ, 2018, pp. 51-80, disponível em: https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U%3d&portalid=30 (consultado a 2/12/2022)

CASTRO, Catarina Sarmento e, "40 Anos de «Utilização da Informática» — O artigo 35.º da Constituição da República Portuguesa", in *e-Pública*, vol. 3, n.º 3, 2016, pp. 42-66

CONLAN, Kevin / BAGGILI, Ibrahim / BREITINGER, Frank, "Anti-forensics; furthering digital forensic science through a new extended, granular, taxonomy", *Elsevier*,

2016, pp. 66-75, disponível em: https://www.sciencedirect.com/science/article/pii/S1742287616300378 (consultado a 14/2/2023)

CORREIA, João Conde, "Prova digital: as leis que temos e as leis que devíamos ter", in *Revista do Ministério Público*, nº139, julho-setembro 2014, pp. 29-59

DIAS, Jorge de Figueiredo

- *Direito Processual Penal*, reimpressão, Coimbra, Coimbra Editora, 2004

- "O Processo Penal Português: problemas e prospetivas", in *Que futuro para o direito processual penal?: Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, (coord. Mário Ferreira Monte, et al.), Coimbra, Coimbra Editora, 2009, pp. 805-819

DUARTE, Maria Luísa, "A discricionariedade administrativa e os conceitos jurídicos indeterminados (contributo para uma análise da extensão do princípio da legalidade)", in *Boletim do Ministério da Justiça*, nº370, 1987, pp. 35-71

FIDALGO, Sónia,

- "A Recolha De Prova Em Suporte Electrónico — Em Particular, A Apreensão De Correio Electrónico", in *Julgar*, nº 38, 2019, pp. 151-160, disponível em http://julgar.pt/wp-content/uploads/2019/05/JULGAR38-08-SF.pdf

- "A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo" in *A Inteligência Artificial no Direito Penal* (coord. Anabela Miranda Rodrigues), reimpressão, 2022, pp. 129-156

FILIOL, Eric, *Computer Viruses: from theory to application,* Springer, 2005, disponível em disponível em: https://repository.root-me.org/Virologie/EN%20-%20Computer%20viruses%20from%20theory%20to%20applications.pdf (consultado a (14/12/2022)

GUTHEIL, Mirja / LIGER, Quentin / HEETMAN, Aurélie / EAGER, James / CRAWFORD, Max, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices", Study for de LIBE Committee, 2017, p. 67, disponível em: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2017)583137 (consultado a 27/12/2022)

HARRIS, Ryan, "Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem", *Elsevier*, 2006, pp. 44-49, disponível em: https://www.researchgate.net/publication/222662987_Arriving_at_an_anti-forensics_consensus_Examining_how_to_define_and_control_the_anti-forensics_problem (consultado em 27/12/2022)

HARTMANN, Arthur, Comentário ao §100a, *Gesamtes Strafrecht Kommentar, StGB / StPO / Nebengesetze – Handkommentar*, (ed. Dieter Rössner), Nomos, 5ª ed., 2022

HASSEMER, Winfried, "Processo penal e direitos fundamentais", in *Jornadas de Direito Processual Penal e Direitos Fundamentais* (coord. Maria Fernanda Palma), Coimbra, Almedina, 2004, pp. 15-25

KOCHHEIM, Dieter, "Onlinedurchsuchung und Quellen-TKÜ in der Strafprozessordnung – Neuordnung der tiefen technischen Eingriffsmaßnahmen in der StPO seit dem 24.8.2017", 2018, disponível em: https://kripoz.de/wp-content/uploads/2018/03/kochheim-onlinedurchsuchung-und-quellen-tkue-in-der-stpo.pdf (consultado a 22/3/2023)

KÖHLER, Marcus, Comentário ao §100b, *Strafprozessordnung: Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen*, Beck'rcheKurz-Kommentare (Bertram Schmitt & Marcus Köhler), Munique, C.H.Beck, 64ª ed., 2021

LEWIS, James A. / ZHENG, Denise E. / CARTER, William A., "The effect of encryption on lawful access to communications and data" A report of the CSIS Tecnhology policy program, 2017, pp. 2 e 3, disponível em: https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data (consultado em 17/2/2023)

LÓPEZ, Isidoro Espín, *Investigación sobre equipos informáticos y su prueba en el proceso penal*, Aranzadi, 2021

MATA-MOUROS, Maria de Fátima, *Juiz das liberdades – desconstrução de um mito do processo penal*, Coimbra, Almedina, 2011

MENDES, Paulo de Sousa,

- "As Proibições de Prova no Processo Penal" in *Jornadas de Direito Processual Penal e Direitos Fundamentais* (coord. Maria Fernanda Palma), Coimbra, Almedina, 2004, pp. 133-154

- "A privacidade digital posta à prova no processo penal" in *Revista Internacional sobre Razonamiento Probatorio*, n.º 2, 2021 pp. 225-250, disponível em: https://dugi-doc.udg.edu/bitstream/handle/10256/19278/11ArticlesPags225-250.pdf?sequence=1&isAllowed=y (consultado a 19/9/2022)

MENKE, Fabiano, "A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão", in *Revista Jurídica Luso-Brasileira*, Ano 5, nº1, 2019, pp. 781-809

MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora, 2010

MILHEIRO, Tiago Caiado, "Buscas online" in *Corrupção em Portugal: avaliação legislativa e propostas de reforma* (org. Paulo Pinto de Albuquerque, et al.), Lisboa, Universidade Católica Editora, 2021, pp. 548-571

NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas em processo penal,* Coimbra, Coimbra Editora, 2011

NUNES, Duarte Rodrigues,

- *Os meios de obtenção de prova previstos na lei do cibercrime,* 1ª ed., Coimbra, Gestlegal, 2018

- *O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada*, 1ª ed., Coimbra, Gestlegal, 2019

PALMA, Maria Fernanda, "Tutela da vida privada e Processo Penal (soluções para o conflito de valores na jurisprudência constitucional)", in *Estudos em memória do Conselheiro Luís Nunes de Almeida*, Coimbra, Coimbra Editora, 2007, pp. 655-672

PEREA, Inmaculada López-Barajas, "Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos" in *Revista de Internet, Derecho y Política*, nº24, fevereiro, 2017, disponível em: https://www.redalyc.org/articulo.oa?id=78850913006 (consultado a 22/3/2023)

PEREIRA, Rui Costa, "A pesquisa de dados informáticos", in *Revista Portuguesa de Ciência Criminal,* ano 31, nº3, setembro-dezembro 2021, pp. 569-608

PLATERO, Paloma Arrabal, "Las diligencias de investigación tecnológica en el proceso penal español", in *Revista de Ciencias Sociales*, numero 76, 2020, disponível em: https://www.researchgate.net/publication/367939659_Las_diligencias_de_investigacion_tecnologicas_en_el_proceso_penal_espanol (consultado a 22/3/2023)

PRADILLO, Juan Carlos Ortiz, "«Hacking» legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática", *Revista de Derecho y Proceso Penal*, nº26, Aranzi, 2011

QUINLAN, Sayako / WILSON, Andi, *A brief history of law enforcement hacking in the United States,* Cybersecurity Initiative, 2016, disponível em: https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf (consultado a 22/03/2023)

RAMALHO, David Silva,

- *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra, Almedina, 2017

- "A investigação criminal na Dark web", in *Revista de Concorrência e Regulação*, ano IV, nº14/15, abril-setembro, 2013, pp. 383-429

- "O uso de *malware* como meio de obtenção de prova em processo penal", in *Revista de Concorrência e Regulação*, ano IV, nº16, outubro-dezembro, 2013, pp. 195-243

RAMOS, Armando Dias, *O Agente Encoberto Digital: meios especiais e técnicos de investigação criminal*, Coimbra, Almedina, 2022

RAUSCHECKER, Markus, "Rule 41 amendments provide for a drastic expansion of government authority to conduct computer searches and should not have been adopted by the supreme court", *Maryland Law Review,* volume 76, issue 4, 2017, disponível em: https://digitalcommons.law.umaryland.edu/mlr/vol76/iss4/8/ (consultado a 22/3/2023)

RODRIGUES, Anabela Miranda, "Política criminal – novos desafios, velhos rumos" in *Liber Discipulorum para Jorge de Figueiredo Dias* (org. Manuel da Costa Andrade, et al.), Coimbra, Coimbra Editora, 2003, pp. 207-234

RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo II, Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010

ROGALL, Klaus, "A nova regulamentação da vigilância das telecomunicações na Alemanha", in *2.º Congresso de Investigação Criminal* (coord. Maria Fernanda Palma, et al.), Coimbra, Almedina, 2011

RUMOLD, Mark, "Assessing the legality and proportionality of communications surveillance in United States law", electronic frontier foundation, 2016, disponível em: https://necessaryandproportionate.org/files/us-en-march2016.pdf (consultado a 22/3/2023)

SANTOS, Cláudia Cruz, "O direito processual penal, as suas finalidades conflituantes e alguns problemas de "burla de etiquetas", in *Estudos em Homenagem do Prof. Doutor Manuel da Costa Andrade*, vol. II, (org. José de Faria Costa, et. al), Coimbra: Boletim da Faculdade de Direito da Universidade de Coimbra, 2017, pp. 815-834

SEIÇA, Alberto Medina, "Legalidade da prova e reconhecimentos «atípicos» em processo penal: notas à margem de jurisprudência (quase) constante", in *Liber Discipulorum para Jorge de Figueiredo Dias* (org. Manuel da Costa Andrade, et al.), Coimbra, Coimbra Editora, 2003, pp. 1387-1421

SILVA, Sandra Oliveira e, "Legalidade da Prova e Provas Proibidas", in *Revista Portuguesa de Ciência Criminal*, Ano 21, nº4, outubro-dezembro 2011, pp. 545-591

SILVA, Germano Marques da, *Direito Processual Penal Português – Noções gerais. Sujeitos processuais e objeto*, Vol. I, 7ª ed., Lisboa, Universidade Católica Editora, 2013

THOMPSON II, Richard M., "Digital searches and seizures: overview of proposed amendments to rule 41 of the rules of criminal procedure", 2016, disponível em: https://sgp.fas.org/crs/misc/R44547.pdf (consultado a 22/3/2023)

VEIGA, Raúl Soares da, "O Juiz de instrução e a tutela de direitos fundamentais", in *Jornadas de Direito Processual Penal e Direitos Fundamentais* (coord. Maria Fernanda Palma), Coimbra, Almedina, 2004, pp. 183-220

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

WINTER, Lorena Bachmaier, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015" in *Boletín del Ministerio de Justicia*, año LXXI, numero 2195, enero de 2017, disponível em: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=R3jUJW0AAAAJ&citation_for_view=R3jUJW0AAAAJ:4OULZ7Gr8RgC (consultado a 22/3/2023)

WOO, Christopher / SO, Miranda, "The case for magic lantern: September 11 highlights the need for increased surveillance", *Harvard Journal of Law & Technology*, volume 15, number 2, 2002, disponível em: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf (consultado a 22/3/2023)

JURISPRUDÊNCIA CITADA

Ac. TC nº91/2023, proc. nº559/2020, Rel. Conselheira Joana Fernandes Costa

Ac. TC nº268/2022, proc. nº828/2019, Rel. Conselheiro Afonso Patrão

Ac. TC nº 324/2013, proc. nº 87/12, Rel. Maria João Antunes

Ac. TC nº607/2003, proc. nº 594/03, Rel. Benjamim Rodrigues

Ac. TRE, proc. 82/20.9PACTX-A.E1, de 25-05-2021, Rel. Martinho Cardoso

Ac. TRE, proc. 2005/08-1, de 07-10-2008, Rel. Martinho Cardoso

Ac. TRG, proc. 19/19.8GCBRG.G1, de 12-04-2021, Rel. Paulo Serafim

Ac. TRL, proc. 368/16.7JAPDL.L1-3, de 09-01-2019, Rel. Nuno Coelho

Ac. TRL, proc. 2903/11.8TACSC.L1-3, de 13-04-2016, Rel. Carlos Almeida

Ac. TRP, proc. 246/12.9TAOAZ-A.P1, de 21-03-2013, Rel. Joaquim Gomes

Ac. TRP, proc. 1001/11.9JAPRT.P1, de , 21-11-2012 Rel. Borges Martins

BVerfG, Decisão do Primeiro Senado, de 27 de fevereiro de 2008 - 1 BvR 370/07

OUTRAS FONTES

Diário da Assembleia da República, I-Série, n.º 102, julho de 2009, disponível em https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684d5a576376524546535353394551564a4a51584a7864576c326279383077716f6c4d6a42545a584e7a77364e764a5449775447566e61584e7359585270646d4576524546535354457 74d6935775a47593d&fich=DARI102.pdf&Inline=true (consultado a 1/5/2023)

Europol/Eurojust, "First report of the observatory function on encryption", janeiro de 2019, disponível em: https://www.eurojust.europa.eu/news/first-europoleurojust-report-encryption-observatory-function#:~:text=On%2011%20January%202019%2C%20Eurojust%2C%20in%20coop

eration%20with,criminal%20use%20of%20encryption%20to%20hide%20illicit%20activities (consultado a 17/2/2023)

Europol/Eurojust, "Common challenges in combating cybercrime", junho de 2019, disponível em: https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf (consultado a 15/2/2023).

Inês Banha "Football Leaks – PJ usou "prova proibida" para chegar a Rui Pinto, acusa advogado", in *Jornal de Notícias*, 6 de janeiro de 2023, disponível em: https://www.jn.pt/justica/pj-usou-prova-proibida-para-chegar-a-rui-pinto-acusa-advogado-15610844.html (consultado em 2/5/2023)

Relatório Anual de Segurança Interna de 2022, disponível em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d (consultado a 5/6/2023)

ÍNDICE GERAL