WASHINGTON TRINDADE DA SILVA JUNIOR

A UTILIZAÇÃO DE *MALWARE* EM INVESTIGAÇÕES CRIMINAIS EM FACE DO ESTABELECIDO PELOS DIREITOS FUNDAMENTAIS

Dissertação com vista à obtenção do grau de
Mestre em Direito na especialidade de Direito Público

Orientador:
Professor Doutor Frederico Lacerda da Costa Pinto, Professor da Faculdade de Direito da Universidade Nova de Lisboa

Dezembro de 2021

WASHINGTON TRINDADE DA SILVA JUNIOR

A UTILIZAÇÃO DE *MALWARE* EM INVESTIGAÇÕES CRIMINAIS EM FACE DO ESTABELECIDO PELOS DIREITOS FUNDAMENTAIS

Dissertação com vista à obtenção do grau de
Mestre em Direito na especialidade de Direito Público

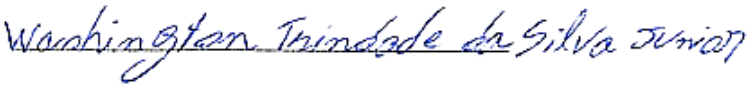
Orientador:
Professor Doutor Frederico Lacerda da Costa Pinto, Professor da Faculdade de Direito da Universidade Nova de Lisboa

Dezembro de 2021

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.

Washington Trindade da Silva Junior



AGRADECIMENTOS

Agradeço aos meus pais e professores.

LISTA DE ABREVIATURAS

AA.VV. — Autores vários

ACPO — Association of Chief Police Officers

Al. — Alínea

Art.º — Artigo

BGH — *Bundesgerichtshof* (Supremo Tribunal Federal Alemão)

BKA — *Bundeskriminalamt* (Polícia Judiciária Federal)

BO2K — *Back Orifice* 2000'

BVerfG — *Bundesverfassungsgericht* (Tribunal Constitucional Federal Alemão)

CCC — *Chaos Computer Club*

CEDH — Convenção Europeia dos Direitos do Homem

CIPA — *Classified Information Procedures Act*

CIPAV— *Computer and Protocol Address Verifier*

CPP — Código de Processo Penal Português

CRFB/88 — Constituição da República Federativa do Brasil de 1988

CRP — Constituição da República Portuguesa

DoS — *Denial of Service*

EUA — Estados Unidos da América

FBI — *Federal Bureau of Investigation*

GPS — *Global Positioning System*

IP — *Internet Protocol*

ISP — *Internet Service Provider*

KLS — *Key Logger System*

LAN — *Local Area Network*

LECrim — *Ley de Enjuiciamiento Criminal*

MAC — *Media Access Control*

N.º — Número

NIST — *National Institute of Standards and Technology*

NIT — *Network Investigative Technique*

NSA — *National Security Agency*

PGP — *Pretty Good Privacy*

RAM — *Random Access Memory*

ROM — *Read-Only Memory*

StPO — Código de Processo Penal Alemão

TCP — *Transmission Control Protocol*

TIC — *Tecnologia da Informação e Comunicação*

TOR — *The Onion Router*

URL — *Uniform Resource Locator*

VoIP — *Voice Over Internet Protocol*

Declaro que a presente dissertação possui um total de 199.704 caracteres.

RESUMO

As novas tecnologias da comunicação e informação e a omnipresença de dispositivos eletrónico-digitais provocam mudanças culturais profundas na sociedade e fazem com que os órgãos de controlo sejam obrigados a adotar métodos de obtenção de fontes de prova diferentes dos que dispunham até há poucos anos, como é o caso do *malware*.

Os ordenamentos jurídicos na República Federativa do Brasil de 1988, assim como em Portugal, não contemplam a utilização do código arbitrário, e, não obstante, verifica-se que esta tarefa legislativa de regulamentação da mencionada ferramenta não poderá ser negligenciada indefinidamente.

Desafios como a utilização, em larga escala, da criptografia e os crimes cometidos constantemente na *dark web* irão, inevitavelmente, impelir estes países a elaborarem uma norma que habilite expressamente o emprego da ferramenta de código malicioso no curso de investigações criminais.

Dada a diversidade de funções que podem ser ativadas sempre que um sistema informático seja penetrado por um código malicioso e dada quantidade massiva de dados de que passarão a dispor os órgãos de controlo durante as investigações de crimes sempre que fizerem uso deste método oculto e extrassensorial, o Poder Legislativo deverá respeitar inquestionavelmente os princípios jurídicos e os direitos fundamentais aplicáveis no momento de erguer um novo diploma jurídico que venha a regulamentar o tema.

A normatização estatal observará a tendência de expansionismo atribuída aos direitos fundamentais, bem como os princípios constitucionais que vincularão a decisão judicial a parâmetros semelhantes.

Palavras-chave: *malware*, métodos ocultos, direitos fundamentais, investigação criminal, tecnologias da informação e comunicação.

ABSTRACT

New communication and information technologies and the ubiquity of electronic-digital devices bring profound cultural changes to society and force control bodies to adopt methods for obtaining sources of evidence different from those available until a few years ago, as is the case with malware.

The legal system in the Federative Republic of Brazil in 1988, as well as in Portugal, does not contemplate the use of the arbitrary code, and, nevertheless, it appears that this legislative task of regulating the aforementioned tool cannot be neglected indefinitely.

Challenges such as the large-scale use of cryptography and the crimes constantly committed on the dark web will inevitably compel these countries to develop a standard that expressly enables the use of the malicious code tool in the course of criminal investigations.

Given the diversity of functions that can be activated whenever a computer system is penetrated by malicious code, and the massive amount of data that the control bodies will have during investigations of crimes whenever they make use of this hidden and extrasensory method, the Legislative Power must maintain unsurpassed respect for the legal principles and fundamental rights applicable at the time of erecting a new legal instrument that will regulate the issue.

State regulation will observe the expansionist tendency attributed to fundamental rights, as well as the constitutional principles that will bind the decision judicial to similar parameters.

Keywords: Malware, occult methods, fundamental rights, criminal investigation, communication and information technologies

INTRODUÇÃO

Para compreender o fenómeno da ferramenta *malware* em investigações criminais públicas, o texto começa por se focar em enquadrar o código malicioso quanto ao conceito, às funcionalidades e às tipologias. No seguimento simples do capítulo, foram indicadas as formas práticas pelas quais o investigador digital poderia introduzir o código arbitrário no interior do sistema de um visado.

Ulteriormente, foi analisada a utilização de código malicioso em investigações criminais nos Estados Unidos da América. Para tal, partiu-se do primeiro caso com repercussão mediática conhecido, tendo, depois, sido analisados outros casos de estudo emblemáticos, e aportando nas alterações legislativas que permitem o emprego da ferramenta além-fronteiras do poder jurisdicional daquela pátria.

Em seguida, analisamos a realidade em Espanha, que, atualmente, regulamenta, de forma bastante completa, a utilização do *malware*, apesar de avaliarmos como passível de críticas o flexível catálogo de crimes e sujeitos expostos pela norma.

Foi trazida também a experiência na Alemanha que lançou marcos jurisprudenciais indispensáveis e que estabeleceu o traço a ser seguido para a compreensão e o limite daquilo que pode ser deferido ao Estado para fins de penetração em sistemas informáticos, inclusive rechaçando plenamente a primeira tentativa de legitimação. Recentemente, o legislador daquela região desincumbiu-se a contento do dever, e foram definidos pela lei fundamentos distintos para a concessão de «vigilância na fonte» e para a busca remota por dados armazenados.

No terceiro capítulo, observamos que, sendo o código malicioso um meio oculto, extrassensorial e que englobará uma série de poderosos recursos concomitantemente, a adoção deste dependerá necessariamente de uma lei expressa, sendo inviável a defesa de que modos de aquisição atípicos não estejam na dependência da norma que os habilite expressamente. Tal regulamentação deverá ser a mais clara possível e observar o princípio da proporcionalidade no que respeita à exigibilidade material, à dimensão de exigibilidade espacial, à dimensão de exigibilidade temporal, e, por fim, à dimensão pessoal. A subsidiariedade que a adoção desta natureza de intrusão importa será levada em consideração num grau elevado e condizente com a respetiva excecionalidade.

Todas as diversas funcionalidades que poderão ser ativadas sempre que o *malware* é instalado poderão entrar em conflito com os direitos fundamentais resguardados por Cartas

Magnas de países democráticos, como sejam: o direito ao sigilo e à proteção das comunicações; o direito à reserva da intimidade; o direito à inviolabilidade do domicílio; o direito à imagem e à palavra; o direito à integridade e confidencialidade dos sistemas informáticos; o direito à autodeterminação informativa.

Avançando no tema, e após a análise de que a maioria das investigações onde se faz uso do código arbitrário deverá recolher dados através da rede mundial de computadores, a pesquisa visa verificar alguns aspetos técnicos relevantes.

Foram examinados, ainda, os pressupostos técnicos para a obtenção de fontes de prova em formato digital. Estas devem seguir precisamente os passos estabelecidos pela ciência forense digital, sob pena de tornar o fruto da investigação criminal inservível em sede de julgamento.

Na sequência do atrás mencionado, o presente estudo aborda algumas das principais medidas antiforenses que são geralmente invocadas para justificar a adoção do código malicioso como medida indispensável aos órgãos de controlo no apuramento da verdade, verificando-se ser o expoente destas medidas de autoproteção a adoção da criptografia, do programa TOR e da esteganografia.

No capítulo final, defendemos que o *malware* não é uma medida regulamentada por lei em Portugal, bem como não é um instrumento típico da República Federativa do Brasil de 1988, e que, ainda assim, foi um instrumento ao qual recorreu a Polícia Federal deste país. Terminamos o presente estudo mencionando o que entendemos serem os requisitos indispensáveis para erguer o regime jurídico deste instrumento, aplicável igualmente a ambas as nações.

1. O *MALWARE*

1.1. Definição do problema

A questão proposta para análise na presente dissertação prende-se com o atual estágio de avanço e penetração social das tecnologias de informação e comunicação, amparadas sempre por uma redução de custos de aquisição e por um maneio a cada dia mais intuitivo, ao dispor de qualquer pessoa, sem limitações de tempo e lugar, que tem vindo a facilitar e a revelar modalidades criminosas[1].

Os reflexos de tais alterações fazem-se sentir em comportamentos individuais e nos mais diversos setores da vida social, tais como a educação, o trabalho, o lazer e as compras[2], com efeitos diretos sobre a instituição do Direito.

É partindo deste ponto que se observa o surgimento do fenómeno do cibercrime e a urgência do Estado em obter provas em formato digital, em especial para a instrução de processos de natureza criminal[3]. Surgem aí realidades técnicas que até há poucas décadas eram desconhecidas e para as quais as adaptações e as analogias com o mundo físico deixaram de ser suficientes.

As interações que o ser humano desenvolve ao longo dos seus dias com os dispositivos de processamento de dados criam e armazenam um grande repertório de informações, por vezes de modo involuntário[4], e potencialmente capazes de reconstruir, em *bits*, desde pensamentos íntimos e perfis completos de um indivíduo[5] até toda uma cadeia de eventos ocorrida durante a realização de um crime.

O facto é que há um interesse dos Estados, em geral, em obter informações em formato digital para uso em investigações policiais, pelo menos desde o final do século passado[6]. A aliança da eventual impossibilidade de acesso ao dispositivo físico que pode conter esta informação com uma possível inexequibilidade da extração de um conjunto de informações

[1]ORTIZ PRADILLO, Juan Carlos. «Remote Forensic Software as a tool for Investigating Cases of Terrorism». *ENAC*. Outubro de 2009, p. 1 — 3

[2]ALBRECHT, Hans-Jorg. «Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos». AA.VV. *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.* Coimbra: Coimbra Editora. 2009, p. 726

[3]CAMPOS, Juliana. *O Malware como Meio de Obtenção da Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 15

[4]LOPES, José Mouraz; CABREIRO, Carlos Antão. «A emergência da prova digital na investigação da criminalidade informática». *Sub judice: Justiça e Sociedade*, n.º 35. Abr. — jun. 2016, p. 74.

[5]RODRIGUES, Benjamim da Silva. *Da Prova Penal — Tomo II. Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*. Lisboa: Rei dos Livros. 2010, p. 472

[6]CARRELL, N. «Spying on the mob: United States V. Scarfo — A constitutional analysis.» *University of Illinois Journal of Law, Technology e Policy*, n.º 1. 2002, p. 199 — 200

constantes de um determinado sistema de processamento de dados revela a necessidade de positivação do método oculto de obtenção de prova chamado de *malware*.

Apesar de não ter sido criado no seio da comunidade de falantes de língua portuguesa, o termo «*malware*» afigura-se o mais preciso para identificar o recurso a ferramentas desta mesma natureza[7], não obstante a existência de uma diversidade de designações usadas a nível internacional. Ainda assim, no presente texto, recorre-se aos termos «código» e «*software* malicioso» para designar *malware*.

Posto isto, cabe concretizar a distinção entre o conceito de pesquisa *on-line* e o recurso a ferramentas de *malware*. De modo abrangente, a doutrina portuguesa segue os ensinamentos de Manuel da Costa Andrade, quando diz que constituem

> «formas de intromissão e abuso dos sistemas informáticos recondutíveis ao conceito de *busca online*. Um conceito compreensivo e abrangente, porventura não inteiramente rigoroso, a que se reconduz um conjunto de intromissões nos sistemas informáticos, feitas através da *internet* e que se actualizam na observação, busca, cópia, vigilância, etc., dos dados presentes naqueles sistemas informáticos»[8].

Apesar disto, o investigador opta por seguir os ensinamentos de David Silva Ramalho[9] quanto à observação de que não se trata propriamente de uma busca, do mesmo modo que uma escuta telefónica não é a mesma coisa que uma busca telefónica, e que o *malware* não necessita de ser instalado *on-line*, assim como a operação de extração de informações poderia ocorrer, igualmente, sem o recurso à rede mundial de computadores.

1.2. Conceito e classificação

O termo «*malware*» resulta da junção do adjetivo «*malicious*» («malicioso») ao substantivo «*software*» («programa»). Refere-se a um programa informático projetado como «um conjunto de instruções executadas em um computador que levam o sistema a fazer algo que o atacante quer que ele faça»[10]. De modo mais complexo, define-se como

> «um programa simples ou autorreplicativo que discretamente se instala em um sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com

[7]Designadamente, os termos «*remote searches*» ou «*remote forensics*», em países de língua inglesa, «*captatore informático*», em Itália, «*registos remotos*», em Espanha, e «*Online-durchsung*», na Alemanha (RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 213).
[8]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, p. 166 (citação *ipsis verbis*)
[9]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 315 – 317
[10]VACCA, John R. *Computer and Information Security Handbook.* Massachusetts: Elsevier. 2012, p. 486

> vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade de sistema ou para assegurar que o utilizador seja incriminado por um crime informático»[11].

O *malware* é, portanto, um código instalado num sistema informático de modo oculto para o utilizador, que, provavelmente, virá a gerar cópias de si mesmo, podendo agir como um agente interno, efetivando os planos de um intruso no sistema operativo da máquina-alvo e levando-a a agir como um servo do atacante.

A maioria do *malware* direciona-se a alguma combinação específica de arquitetura do computador e sistema operativo, e, por vezes, até a um programa ou aplicação específicos.

A miríade de capacidades de um código de programa malicioso, ou seja, daquilo que pode ser efetivado quando um atacante faz uso de um *malware* e das respetivas capacidades de ação no interior de um sistema operativo, só tem limites na imaginação e, em certa medida, nos conhecimentos técnicos dos respetivos criadores. Ressalta-se, porém, que se disponibilizam na *Internet* ferramentas para que utilizadores com pouca destreza consigam elaborar os seus próprios *softwares* maliciosos[12].

Em regra geral, um programa de código malicioso tem, possivelmente, a capacidade de excluir arquivos de um disco rígido; usar o computador infetado para se espalhar para outros computadores que com este estejam ligados em rede ou para os contactos presentes numa lista de *e-mail*s; monitorizar todas as teclas pressionadas pelo utilizador; verificar informações sobres as páginas consultadas na *Web*; enviar ao atacante vídeos de tudo o que se passa no ecrã do computador infetado; dar instruções ao computador para efetuar ações com um nível de autorização idêntico ao detido pelo próprio utilizador que detenha permissões de administrador, inclusivamente acionando partes do *hardware,* como a câmara e o microfone[13]. Tem ainda a capacidade de furtar ficheiros pessoais ou sobrescrever permanentemente os dados no disco rígido[14], bem como, no interior do computador pessoal do alvo, carregar ficheiros ilícitos, como sejam dados roubados, imagens com conteúdo de pornografia infantil ou até um novo tipo de *malware*. Pode, ainda, usar o sistema informático atacado como base para novas incursões semelhantes.

É, pois, possível afirmar que um programa malicioso é capaz de executar qualquer atividade que os equipamentos de processamento de dados modernos estão habilitados a

[11]FILIOL, Eric. *Computer viruses: from theory to applications*. França: Spienger. 2005, p. 83
[12]AYCOCK, John. *Computer Viruses and Malware.* EUA: Springer. 2006, p. 28
[13]RAMALHO, David Silva. «O uso de *malware* como meio de obtenção de prova em processo penal». *Revista de Concorrência e Regulação*, Ano IV, n.º 16. Out. — dez. de 2013, p. 207
[14]SINROD, Eric J.; REILLY, William P. «Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws». *Santa Clara Computer and High Technology Law Journal,* vol. 16, n.º 2. 2000, p. 218

desempenhar e permite vislumbrar que as funcionalidades evoluirão de modo a acompanharem o crescente desenvolvimento das tecnologias de informação e comunicação.

Uma vez salientados o conceito e as potencialidades do *malware*, cabe agora analisar em que tipos se divide o *malware*, de acordo com o conjunto de funcionalidades e características comuns apresentadas por cada espécie, já que os códigos maliciosos podem ser divididos em categorias, de acordo com o respetivo método de operação.

O investigador sustenta, em conformidade com os ensinamentos de David Silva Ramalho, que poderá existir sobreposição de conceitos, como consequência da constante evolução do programa informático malicioso e das divergências encontradas em sede de literatura especializada, no que tange a características pertencentes a cada um dos tipos a seguir discriminados[15].

É possível definir um vírus como um componente de um código que se autorreproduz e se liga a outros programas, e que, geralmente, requer interação humana para se propagar[16].

O código arbitrário que integra a categoria de vírus não funciona como um programa executável autónomo, sendo necessário que se ligue ao código de um *software*[17] hospedeiro, que pode ser um ficheiro executável ou mesmo um ficheiro de dados.

Esta ligação parasitária ocorre quando o vírus se anexa no início ou no final do código do hospedeiro ou promove a substituição do código desse programa ou arquivo pelo respetivo código. Nestas situações, a criação de cópias automáticas será feita pelo vírus apenas quando o utilizador correr o programa hospedeiro[18].

Há, pois, a possibilidade de o código malicioso de natureza viral estar acondicionado em diversos pontos da memória do computador. É possível que o vírus seja acondicionado em conjunto com instruções do setor de inicialização de um disco rígido que informam como o computador deve inicializar o sistema operativo.

É importante observar que nem todos os vírus causam danos ao seu hospedeiro, pois podem ter sido desenvolvidos para fins não prejudiciais. Podem, por exemplo e simplesmente, estar orientados para exibir uma mensagem em determinada data[19].

[15]RAMALHO, David Silva. «O uso de *malware* como meio de obtenção de prova em processo penal». *Revista de Concorrência e Regulação*, Ano IV, n.º 16. Out. — dez. de 2013, p. 198
[16]VACCA, John R. *Computer and Information Security Handbook.* Massachusetts: Elsevier. 2012, p. 295
[17]CORREIA, Miguel Pupo; SOUSA, Paulo Jorge. *Segurança no Software.* Lisboa: FCA, 2.ª Ed. 2017, p. 21
[18]Idem
[19]SINROD, Eric J.; REILLY, William P. «Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws». *Santa Clara Computer and High Technology Law Journal*, Vol. 16, n.º 2. 2000, p. 216

Infelizmente, esta não é a regra, e os vírus têm, a maior parte das vezes, funções perniciosas. A parte do vírus que contém esta finalidade denomina-se «carga útil», e corresponde ao dano que este *malware* promove[20].

O *worm* define-se como um código autorreplicativo que se propaga por uma rede, geralmente sem necessidade de interação humana[21]. Além das redes locais (LAN) por onde o *worm* instantaneamente se propaga, a rede maioritariamente usada para a infeção é a *Internet*, ainda que possam ser usadas outras redes, como o *Bluetooth*.[22,23]

O que distingue um *worm* de um vírus é o facto de o primeiro se espalhar pela rede, além de não precisar de estar anexado a um programa ou arquivo para infetar um novo sistema operativo[24].

No caso dos *worm*s, o código malicioso explora vulnerabilidades no *software* do utilizador-alvo e penetra de modo automatizado[25], após localizar, com sucesso, uma falha de segurança na configuração[26].

O objetivo mais comum do *worm* é deixar uma cópia de si mesmo noutros computadores que possa invadir, e, logo depois, executar a sua carga útil. Esta poderá, por exemplo, causar danos no conteúdo de ficheiros e/ou proporcionar a tomada de controlo de todo o sistema operativo, promover ataques de negação de serviço (DoS) etc.[27]

A primeira vez que um *worm* foi lançado e se proliferou livremente pela rede mundial de computadores, causando prejuízos financeiros[28], foi em 1988. Este *malware*, criado por Robert Morris Jr., que acabou por receber o nome do seu produtor, pretendia somente medir o tamanho da Internet naquela época, mas acabou por causar um ataque de negação de serviço (DoS) por congestionamento da rede[29], fugindo ao controlo do seu produtor.

Os programas maliciosos chamados «cavalos de Troia» receberam esta designação por referência ao episódio da Guerra de Troia, descrito na *Ilíada*, segundo o qual os gregos construíram a estátua de um cavalo que os troianos tomaram como oferenda e levaram para

[20]SINROD, Eric J.; REILLY, William P. «Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws». *Santa Clara Computer and High Technology Law Journal*, Vol. 16, n.º 2. 2000, p. 216
[21]VACCA, John R. *Computer and Information Security Handbook.* Massachusetts: Elsevier. 2012, p. 295
[22]CORREIA, Miguel Pupo; SOUSA, Paulo Jorge. *Segurança no Software.* Lisboa: FCA, 2.ª Ed. 2017, p. 21
[23]BICKFORD, Jeffrey et al. «Rootkits on smart phones: Attacks, implications and opportunities». *Proceedings of the 11th International Workshop on Mobile Computing Systems and Applications.* Annapolis: Maryland. 2010, p. 1
[24]FILIOL, Eric. *Computer viruses: from theory to applications.* França: Spienger. 2005, p. 141
[25]Europol. *Malware Basics.* [Obtido de https://www.europol.europa.eu/sites/default/files/documents/malwarebasicscomplete.pdf (consultado a 20/06/2021)]
[26]CORREIA, Miguel Pupo; SOUSA, Paulo Jorge. *Segurança no Software.* Lisboa: FCA, 2.ª Ed. 2017, p. 21
[27]GRAHAM, James et al. *Cyber Security Essentials.* Boca Roton: Taylor and Francis. 2011, p. 195
[28]BRITZ, Marjie T. *Computer Forensics and Cyber Crime: An Introduction* — 3rd ed. New Jersey: Prentice Hall. 2013, p. 55
[29]GRAHAM, James et al. *Cyber Security Essentials.* Boca Roton: Taylor and Francis. 2011, p. 195

dentro das suas muralhas. No interior da estátua, encontravam-se soldados, que, uma vez obtido o acesso ao interior da cidade fortificada, encetaram um ataque noturno que culminou com a vitória grega.

Em conformidade com a situação que inspirou o nome, o cavalo de Troia consiste num invólucro ou um método de entrega, mais do que um programa malicioso por si, dentro do qual pode estar contido um vírus, um *worm*, um *spyware* etc.[30] O objetivo é permitir ultrapassar furtivamente barreiras de segurança como, por exemplo, uma *firewall*, e, com a ajuda do próprio utilizador incauto, instalar o programa na máquina do alvo sem que este disso se aperceba.

Um exemplo famoso foi o Back Orifice 2000' (BO2K), um cavalo de Troia que, uma vez instalado no computador da vítima, permitia de imediato ao *hacker* executar comandos do sistema, redirecionar o tráfego de rede e reconfigurar o computador da vítima. Se o computador estivesse em rede, o *hacker* poderia obter acesso a essa rede[31].

O cavalo de Troia é um código simples que não se consegue autorreplicar[32], e que é constituído por duas partes: o módulo do servidor e o módulo do cliente. O módulo de servidor, uma vez instalado de modo sub-reptício[33], confere ao invasor acesso silencioso a todos os elementos do computador do alvo. O invasor pode usá-lo para se conectar ao computador da vítima secretamente, por meio de redes, criando *backdoors*[34], com o intuito de contornar as medidas normais de segurança[35]. O módulo de servidor é um programa escondido noutro programa de aspeto lícito e aparentemente útil para o utilizador. Depois de esse programa supostamente inofensivo ser executado pelo menos uma vez, será instalada a componente do servidor do programa cavalo de Troia, sem que o utilizador disto se aperceba.

---

[30]SHEETEZ, Michael. *Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers.* New Jersey: John Wiley & Sons. 2007, p. 77

[31]SINROD, Eric J.; REILLY, William P. «Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws». *Santa Clara Computer and High Technology Law Journal*, Vol. 16, n.º 2. 2000, p. 223 — 224

[32]SHEETEZ, Michael. *Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers*. New Jersey: John Wiley & Sons. 2007, p. 76

[33]BRENNER, Susan W. *Cybercrime — Criminal Threats from Cyberspace.* California: ABS-CLIO, LLC. 2010, p. 105

[34]Segundo o documento da Europol, *Malware Basics*, uma *backdoor* consistiria em algo que permite o acesso remoto e não autorizado a um sistema informático. As *backdoors* podem ser detetadas (caso já existam) ou instaladas por meio de outro *malware*. dando controlo quase total ao atacante, que pode executar uma ampla gama de ações: monitorizar, interferir, intercetar, modificar, etc. Europol. *Malware Basics.*
[Obtido de https://www.europol.europa.eu/sites/default/files/documents/malwarebasicscomplete.pdf (consultado a 20/06/2021)]

[35]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 320

Com a criação de *backdoors*, os computadores infetados podem ser controlados remotamente. O controlo da máquina permite que o invasor lance uma grande variedade de ações ofensivas, dependendo da natureza do *software* malicioso: reiniciar o computador; transferir arquivos; destruir dados; obter senhas de acesso para páginas exclusivamente individuais da rede mundial de computadores, tais como *webmails*; instalar código malicioso de outros formatos; servir como meio para que o atacante visite *sites* na rede mundial usando o endereço de IP (*Internet Protocol*) do utilizador-vítima, camuflando, assim, quaisquer atividades criminosas que possa vir a cometer durante a navegação[36].

As chamadas *logic bomb*s, ou «bombas-relógio», são, historicamente, um dos primeiros formatos de código malicioso, instaladas como um código inativo que pode ser acionado numa data futura, no seguimento de um evento específico. São um tipo de *malware* não replicativo[37], concebido com uma função perniciosa para o sistema informático do utilizador. O gatilho que desencadeia a carga útil das *logic bombs* pode ser uma data e hora específicas ou mesmo um número cumulativo de inicializações do sistema[38].

Muitos programadores insatisfeitos implantaram bombas-relógio como forma de retaliação dos respetivos empregadores. Foi o caso de um administrador de rede que, na iminência de ser despedido, projetou e instalou uma *logic bomb* que, diariamente, verificava se o nome do administrador ainda constava da lista de pagamentos no computador do departamento de recursos humanos. Após o seu despedimento, a *logic bomb* criptografou todos os discos rígidos da empresa, incluindo os *backups*, por meio de uma chave secreta aleatória. Pela sua natureza, ninguém na empresa, nem mesmo o próprio ex-administrador, conseguiu descodificar a chave, e todos os dados da empresa foram definitivamente perdidos[39].

Por *spyware*, entende-se qualquer programa informático que reúne informações sobre uma pessoa ou organização sem o conhecimento ou consentimento[40] destes. Todo o *spyware* monitoriza, em algum nível, a utilização que se faz de um computador, sendo projetado assim para a extração e o roubo de dados[41].

---

[36]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 320
[37]Idem
[38]ERBSCHLOE, Michael. *Trojans, Worms and Spyware — A Computer Security Professional's Guide to Malicious Code*. EUA: Elsevier. 2005, p. 25
[39]FILIOL, Eric. *Computer viruses: from theory to applications*. França: Spienger. 2005, p. 99
[40]ERBSCHLOE, Michael. *Trojans, Worms and Spyware — A Computer Security Professional's Guide to Malicious Code.* EUA: Elsevier. 2005, p. 25
[41]VACCA, John R. *Computer and Information Security Handbook*. Massachusetts: Elsevier. 2012, p. 57

Um *spyware* pode infetar um sistema operativo através de diversos mecanismos ocultos, inclusive pelo seu carregamento em cavalos de Troia[42]. Entre as diversas funções que um *spyware* pode desempenhar, o investigador salienta o *adware*, que gera *pop-ups* de programas que comunicam informações sobre as atividades de um utilizador conectado na rede mundial de computadores a um sistema remoto, sem o seu conhecimento.

Esta forma de *malware* inclui também: programas *sniffer*, que possibilitam intercetar, em tempo real, os dados que entram e saem de um determinado computador ligado em rede; *keyloggers*, que registam as teclas premidas pelo utilizador; *screenloggers*, que capturam a posição do cursor do rato e o ecrã apresentado no monitor, sempre que houver um clique no rato; *cookies*, que registam os hábitos de visualização do utilizador na *Internet*; e *web bugs*, que são incorporados em páginas da *Web* ou no *e-mail* e obtêm informações sobre a data e hora dos acessos, bem como o endereço IP e o tipo de navegador do computador de acesso[43].

Formas mais interventivas de *spyware* podem alterar as configurações do computador, redefinir as páginas iniciais e redirecionar o navegador para *sites* indesejados[44].

Como forma de permanecer no sistema informático onde foi instalado e de evitar a deteção por programas *anti-spyware*, existe a possibilidade de este *malware* promover a sua atualização a partir do sistema informático infetado[45].

No entanto, nem sempre o *spyware* será instalado num computador de modo ilegítimo, e pode ser colocado num sistema operativo para reunir informações sobre um utilizador. Estas informações, por sua vez, podem ser posteriormente vendidas a anunciantes e a outras partes interessadas. Trata-se de uma situação que prevalece amplamente em computadores pessoais. As informações reunidas pelo *spyware* costumam ser combinadas com as de outros bancos de dados para criar perfis de indivíduos, famílias etc.[46], que são, depois, usados principalmente para fins de publicidade e propaganda, com ou sem o consentimento do proprietário do computador.

Os *rootkits* são uma forma de *software* malicioso que atinge os seus objetivos por infeção do sistema operativo. Consistem em programas informáticos furtivos, que permitem que o invasor mascare a sua presença e, de seguida, obtenha acesso privilegiado ao sistema

[42]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 321
[43]CLOUGH, Jonathan. *Principles of Cybercrime*. Cambridge: Cambridge University Press. 2010, p. 36
[44]VACCA, John R. *Computer and Information Security Handbook.* Massachusetts: Elsevier. 2012, p. 57
[45]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 321
[46]ERBSCHLOE, Michael. *Trojans, Worms and Spyware — A Computer Security Professional's Guide to Malicious Code*. EUA: Elsevier. 2005, p. 25

operativo de uma máquina[47], que é considerado a base da computação confiável. Consequentemente, podem manter o controlo a longo prazo das máquinas infetadas[48].

A maioria dos *rootkits* permite que um invasor faça *login* num sistema sem que se gerem registos da sua presença. Através de um mecanismo semelhante, também permitem que um invasor oculte a utilização que faz da rede do sistema. Podem ser usados para ocultar arquivos e processos, ou seja, ordens enviadas ao sistema de processamento de dados, em espaços apenas acessíveis ao utilizador mal-intencionado, instalar cavalos de Troia e desativar *firewall*s e antivírus.

Na literatura, é habitual dividir os *rootkits* em dois níveis: utilizador e *kernel*[49]. No nível de utilizador, o *rootkit* promove, normalmente, a falsificação de um único processo de cada vez, para ocultar informações. No nível de *kernel*, esta forma de *malware* pode proceder a alterações em estruturas críticas da memória, para ligar e modificar certas funções de ordens dadas ao sistema[50]. Isto tornará mais difícil a deteção por meio de antivírus e *anti-spyware*.

Um *bot* é um sistema informático que, ao infetar o computador-alvo, permite que este seja controlado remotamente. O invasor explora, assim, os pontos fracos de segurança, geralmente num dispositivo conectado à *Internet*, para nele colocar pequenos programas chamados *deamons*, desconhecidos do terceiro[51].

A rede que se constitui por este conjunto de máquinas afetadas por um *malware* é conhecida como *botnet*. Uma *botnet* pode incluir um enorme número de computadores pessoais infetados, tornados uma entidade única a serviço do atacante[52].

Cada vez mais, as redes ponto a ponto estão a ser usadas para lançar tais ataques, tendo em consideração que, para desmontar uma agressão desta natureza, é necessário identificar a máquina de que partem os comandos, e a função da mencionada rede é dificultar o seu desligamento, por não existir um ponto único de controlo.

---

[47]BRENNER, Susan W. «At the light speed: attribution and response to cybercrime/terrorism/warfare». *Journal of Criminal Law and Technology*, Vol. 97, n.º 2. 2007, p. 380

[48]BICKFORD, Jeffrey et al. «Rootkits on smart phones: Acks, implications and opportunities». *Proceedings of the 11th International Workshop on Mobile Computing Systems and Applications.* Annapolis: Maryland. 2010, p. 5

[49]O *kernel* é muitas vezes considerado o cérebro do computador, consistindo na ligação entre o processamento de dados e as aplicações instaladas.

[50]GRAHAM, James et al. *Cyber Security Essentials.* Boca Roton: Taylor and Francis. 2011, p. 219 — 223

[51]CLOUGH, Jonathan. *Principles of Cybercrime.* Cambridge: Cambridge University Press. 2010, p. 35

[52]ZARAGOZA TEJADA, Javier Ignacio. *Investigación tecnológica y derechos fundamentales: Comentarios a las modificaciones introducidas por la ley 13/2015 (Gran Tratado n.º 928). (Spanish Edition)* — 1.ª Ed. Aranzadi/Cívitas. 2017, p. 495 (Versão eletrónica)

Os criadores de códigos maliciosos tornaram-se sofisticados, ao combinar as características e capacidades de vários tipos de ameaças[53]. As *blended threats* (ameaças combinadas) incluem, assim, mais de uma espécie de *malware*. Uma *blended threat* é, geralmente, capaz de se mover pela *Internet* com recurso a vírus veiculados por *e-mail*, ou *worms*. Um ataque desta natureza poderia resultar na instalação de um cavalo de Troia num computador[54], usando como gatilho uma ação da aplicação de *e-mail* ou uma ação de navegação na *Internet*.

1.3. Métodos viáveis para a instalação

No que respeita ao modo de instalação, o *software* malicioso pode ser levado para o interior de um sistema informático de diversos modos, todos hábeis a servir o propósito de contaminar um equipamento de processamento de dados. São três, os modos mais usuais[55] e, historicamente, mais utilizados para difundir *malware*.

O primeiro mecanismo de infeção de que se tem registo ocorre através de um suporte removível. Este método de entrega foi o mais comum para a difusão dos diversos tipos de *malware* durante várias décadas, e a única forma de atingir um computador pessoal, com a introdução de um código malicioso durante a denominada «Era Clássica» (1960—1970), antes do advento da popularização da *Internet*. Num segundo momento evolutivo, nomeado pela literatura especializada como «Era da Disquete» (1980—1990)[56], observou-se uma forte propagação de *malware* por meio de dispositivos removíveis fabricados para armazenar dados, apesar de ainda se tratar de um modo lento de difusão, quando comparado com o mesmo fenómeno que ocorre atualmente na *Internet*.

Os criadores de código malicioso tinham consciência da tendência dos utilizadores de computadores pessoais para partilharem ficheiros usando dispositivos como disquetes, *pen drives* USB, CD etc. Quando acoplados a um sistema informático, tais dispositivos contaminados no seu setor de inicialização com *malware* autorreplicativo[57] transferem-no para os setores da memória do computador em que se encontram. Caso um atacante pretenda

---

[53]ERBSCHLOE, Michael. *Trojans, Worms and Spyware — A Computer Security Professional's Guide to Malicious Code*. EUA: Elsevier. 2005, p. 24

[54]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 319

[55]RAMALHO, David Silva. «O uso de *malware* como meio de obtenção de prova em processo penal». *Revista de Concorrência e Regulação,* Ano IV, n.º 16. Out. — dez. de 2013, p. 205

[56]BRITZ, Marjie T. *Computer Forensics and Cyber Crime: An Introduction — 3rd ed.* New Jersey: Prentice Hall. 2013, p. 78

[57]RAMALHO, David Silva. «O uso de *malware* como meio de obtenção de prova em processo penal». *Revista de Concorrência e Regulação,* Ano IV, n.º 16.Out. — dez. de 2013, p. 205

contaminar um único sistema operativo, este método revela segurança, haja vista que a integridade de outra máquina não seja atingida no processo e os danos sejam localizados e correspondentes ao alvo inicialmente visado.

O segundo método de instalação de um código malicioso surgiu após o advento da *Internet*, e diz respeito ao *drive-by-download*[58]. O processo de entrega destes códigos para o interior de um computador ocorre quando o utilizador do sistema informático acede a uma página da rede mundial de computadores, aparentemente inócua, mas que, na verdade, provém de servidores que contêm códigos maliciosos.

O utilizador poderia, por exemplo, navegar por páginas de notícias da *Web* e clicar numa hiperligação referente a um anúncio publicitário, que seria direcionado para um servidor da *Web* comprometido por *malware*. Este, por sua vez, infetaria o sistema operativo do utilizador com esse código, de forma automática, explorando vulnerabilidades na configuração do equipamento informático ou no navegador usado para abrir aquela página *Web*[59].

Os sítios eletrónicos legítimos são muito apelativos para o atacante, na medida em que a maioria dos internautas manifesta relutância em aceder a páginas suspeitas na *Internet*, sentindo-se sempre seguros quando navegam por páginas legítimas[60].

Ao contrário do que sucede com o primeiro método, pode observar-se que não é possível controlar a quantidade de sistemas que serão infetados enquanto a página da *Internet* que contém código malicioso estiver operacional para disseminar o código malicioso.

Existe ainda um terceiro modelo de introdução de *malware*: por meio de *download* voluntário, ou seja, através do *download* de um determinado ficheiro contendo um código arbitrário. Atualmente, é mais prático partilharmos ficheiros através da *Internet*, anexando os mesmos em *e-mails* ou aplicações de mensagens instantâneas, para que possam ser descarregados. E, como salvaguarda, na senda do que refere David Silva Ramalho, podemos ainda ser levados a proceder voluntariamente ao *download* de uma falsa atualização de *software* legítimo[61].

[58]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 323
[59]CASEY, Eoghan; DAYWALT, Christopher. «Computer Intrusion». *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet* — 3.ª ed. Academic Press/Elsevier, 2011, p. 377
[60]VACCA, John R. *Computer and Information Security Handbook.* Massachusetts: Elsevier. 2012, p. 48, 58
[61]RAMALHO, David Silva. «O uso de *malware* como meio de obtenção de prova em processo penal». *Revista de Concorrência e Regulação,* Ano IV, n.º 16. Out. — dez. de 2013, p. 205

Estando o ficheiro na memória do sistema, ao ser executado, o *malware* será instalado e tratará de «desativar o antivírus ou substituir um programa normalmente em execução»[62].

Nestas circunstâncias, não será possível determinar a quantidade precisa de sistemas informáticos comprometidos com o código arbitrário instalado remotamente, podendo lesar um número indeterminado de indivíduos.

Um método ainda pouco explorado, registado pela universidade de Toronto, é conhecido como o «clique zero». É um método segundo o qual o *malware* é instalado em sistemas operacionais conectados à Internet bastando a realização de uma chamada de voz sobre IP (VoIP) para uma aplicação como o *WhatsApp*, em que o utilizador não necessita de levar a cabo nenhuma ação para que a instalação seja efetivada. Tal recurso foi atribuído especificamente ao *malware* conhecido como Pegasus, da empresa israelita NSO Group, que comercializa ferramentas de vigilância destinadas a entidades governamentais[63].

[62]BATISTA, Lydie Jorge. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Dissertação de Mestrado em Ciências Jurídico-Forenses. Faculdade de Direito — Universidade de Lisboa. 2018, p. 31

[63]MARCZAK, Bill et al. (2020). «The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit». *Citizen Lab Research Report, n.º 135*. [Disponível em: https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/ (acedido pela última vez em 06/06/2021) e https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-pernicious-invisibility-of-zero-click-mobile-attacks/?sh=4ae65d5c3079 (acedido pela última vez em 06/06/2021)]

2. O RECURSO AO *MALWARE* NO DIREITO COMPARADO

2.1. A admissibilidade do *malware* nos Estados Unidos da América (EUA)

A opção pela avaliação da admissibilidade de recurso a *software* malicioso nos EUA justifica-se, sobretudo, pelo longo histórico da sua utilização por parte das forças de segurança norte-americanas.

O primeiro caso registado de uso desta ferramenta por parte das forças de segurança que trouxe repercussões aconteceu em Nova Jérsia. Partindo de notícias obtidas por informantes acerca da prática dos crimes de jogo ilegal e agiotagem, agentes do FBI (*Federal Bureau of Investigation*) obtiveram, em janeiro de 1999, um mandado judicial para realizarem buscas no escritório gerido por Nicodemo S. Scarfo e Frank Paolercio[64]. Foi, assim, localizado um ficheiro armazenado no computador pessoal de Scarfo, com o nome «*Factors*», que levantou fortes suspeitas relativamente ao conteúdo. Era possível que contivesse material incriminatório, pois estava protegido com a criptografia fornecida por um *software* gratuito chamado *Pretty Good Privacy* (PGP), indecifrável sem a palavra-passe, na posse unicamente dos proprietários do ficheiro[65].

Em maio de 1999, os agentes do FBI solicitaram e obtiveram dois novos mandados judiciais. O primeiro deles previa uma autorização para a entrada e reentrada secretas no escritório no prazo de 30 dias[66], tantas vezes quantas se revelassem necessárias para a efetivação do objetivo constante da ordem[67]. O segundo previa a instalação, no computador de Scarfo, de um sistema complexo, que incluía componentes de *hardware*, *software* e/ou *firmware,* designado por *Key Logger System* (KLS)[68], e tinha a função de registar todas as teclas premidas no computador, desde que o *modem* de acesso à *Internet* estivesse desligado[69]. Deste modo, o *malware* de natureza *keylogger* instalado não intercetava

[64]MOHAY, George; ANDERSON, Alison; COLLIE, Byron; VEL, Oliver de; MCKEM-MISH, Rod. *Computer and Intrusion Forensics*. Massachusetts: Artech House, Inc. 2003, p. 120
[65]CARRELL, N. «Spying on the mob: United States V. Scarfo — A constitutional analysis.» *University of Illinois Journal of Law, Technology e Policy*, n.º 1. 2002, p. 199 — 200
[66]Idem
[67]BATISTA, Lydie Jorge. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Dissertação de Mestrado em Ciências Jurídico-Forenses. Faculdade de Direito — Universidade de Lisboa. 2018, p. 153.
[68]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 311
[69]SHEETEZ, Michael. *Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers.* New Jersey: John Wiley & Sons. 2007, p. 142

comunicações escritas, mas somente os dados destinados a serem inseridos e/ou armazenados na memória do computador, não apresentando confronto com o *Wiretap Act*[70].

Destarte, após recolherem 45 páginas com as teclas premidas pelos suspeitos, os agentes do FBI identificaram como palavra-passe que desencriptou o ficheiro acima mencionado o número do registo prisional do pai de Scarfo[71].

No dia 21 do mês de junho de 2000, Scarfo e Paolercio foram acusados formalmente pelos crimes de jogo ilegal e agiotagem[72]. A defesa requereu que fossem revelados os detalhes técnicos do funcionamento do KLS. No entanto, o Governo dos EUA recusou, e o Poder Judiciário garantiu ao Departamento de Justiça a proteção do *Classified Information Procedures Act* (CIPA), sob a alegação de que a publicitação dos detalhes técnicos do KLS traria riscos para a segurança nacional. A defesa somente conseguiu obter um resumo das funcionalidades do *keylogger*[73].

O advogado de defesa de Scarfo alegou que as provas eram inadmissíveis, afirmando que os agentes haviam extrapolado os limites do mandado, uma vez que este apenas autorizava a recolha de informações relacionadas com a palavra-passe, e convertido a diligência numa busca exploratória, vedada pela Quarta Emenda constante da Constituição norte-americana. Argumentou ainda que a acusação estaria obrigada a fornecer os detalhes do KLS, com base, por um lado, em precedentes que estabeleciam a necessidade de a acusação revelar os testemunhos prestados antes do inquérito em julgamento e, por outro, que a ferramenta *keylogger* havia intercetado comunicações entre os acusados[74].

O Tribunal Distrital de Nova Jérsia rebateu todos os argumentos, defendendo que as palavras recolhidas que não constituíam a chave para desencriptar o ficheiro não seriam relevantes, não originando consequências processuais; que não havia similaridades relevantes entre o caso protagonizado por Scarfo e o precedente invocado; e, por fim, tomou como confiável a afirmação do FBI de que nenhuma comunicação fora intercetada, ainda que apenas fosse dado a conhecer um resumo das funcionalidades do KLS[75].

---

[70]SHEETEZ, Michael. *Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers.* New Jersey: John Wiley & Sons. 2007, p. 142

[71]MOHAY, George; ANDERSON, Alison; COLLIE, Byron; VEL, Oliver de; MCKEM-MISH, Rod. *Computer and Intrusion Forensics*. Massachusetts: Artech House, Inc. 2003, p. 223 — 224

[72]Idem; p. 225

[73]Idem; p. 226

[74]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 312

[75]BATISTA, Lydie Jorge. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Dissertação de Mestrado em Ciências Jurídico-Forenses. Faculdade de Direito — Universidade de Lisboa. 2018, p. 153.

Este caso retrata como o Governo do EUA tem vindo sistematicamente a colocar armadilhas para intercetar informações e comunicações desde há várias décadas[76].

Um antecessor dos programas usados nos últimos vinte anos pelas forças de segurança norte-americanas com a finalidade de exercer vigilância foi o *Carnivore* (também conhecido como DCS-1000), um *software* (*Packet Sniffer*) que tem a capacidade de detetar pacotes de dados enviados de um computador para outro, através de um servidor[77]. Dito de outro modo, trata-se uma ferramenta do FBI que conduz a vigilância direta sobre a *Internet*, uma armadilha que consegue ler o tráfego enquanto está em curso a transmissão.

Apesar de se tratar de um método oculto de investigação criminal, não podemos classificar este *software* como *malware*, já que dispensa a instalação num dispositivo para obter as informações que entram e saem de um processador de dados.

No ano de 2001, uma investigação jornalística trouxe ao conhecimento público a utilização por parte do FBI de um *malware* que ficou conhecido como *Magic Lantern*[78]. Esta ferramenta teria como utilidade facilitar a aquisição de chaves criptográficas, como as obtidas no caso Scarfo, já que o *software* poderia ser instalado sem que o investigador tivesse acesso físico ao computador de destino, podendo ser entregue como um anexo de *e-mail* contendo o código arbitrário ou fazendo uso de um *exploit*[79]. De entre as funcionalidades disponíveis, podia registar as teclas premidas, enviando-as aos agentes sempre que o computador apresentasse uma conexão com a *Internet*[80].

Ciente da possibilidade de deteção do *Magic Lantern* por antivírus, o Governo dos EUA solicitou às empresas dedicadas a este nicho de mercado que desenhassem estes produtos de modo a não interferir no funcionamento do seu código malicioso[81].

Em 2007, surgiram na imprensa informações de que o FBI havia solicitado um mandado judicial no âmbito de um processo que investigava ameaças de bomba contra uma escola do estado de Washington, detetadas com recurso a um *malware* chamado *Computer*

[76]WOO, Christopher; SO, Miranda. «The Case for Magic Lantern: September 11 Highlights — The need for Increased Surveillance». *Harvard Journal of Law & Technology*, Vol. 15, n.º 2. 2002, p. 521 — 538.
[77]KERR, Orin S. «The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"». *Connecticut Law Review*, Vol. 33. 2001, p. 622
[78]THOMPSON II, Richard M. *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure*. 8 de setembro de 2016, p. 2 – 3. Obtido de Congressional Research Service: https://fas.org/sgp/crs/misc/R44547.pdf
[79]Segundo Miguel Pupo Correia e Paulo Jorge Sousa, um *exploit* é um trecho de código capaz de ativar determinada vulnerabilidade num pacote de *software* (CORREIA, Miguel Pupo; SOUSA, Paulo Jorge. *Segurança no Software*. Lisboa: FCA, 2.ª Ed. 2017, p. 15)
[80]WOO, Christopher; SO, Miranda. «The Case for Magic Lantern: September 11 Highlights — The need for Increased Surveillance». *Harvard Journal of Law & Technology*, Vol. 15, n.º 2. 2002, p. 521 — 538.
[81]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 326

and Protocol Address Verifier (CIPAV)[82], desenvolvido para agir concomitantemente com o *Magic Lantern*[83].

As referidas ameaças teriam partido de diversos endereços de *e-mail* criados a partir de números IP localizados em Itália, entre eles o do Instituto de Física Nuclear da Itália. O primeiro destes *e-mail*s informava que, antes de as bombas serem acionadas, os servidores de *e-mail* do distrito escolar ficariam fora de serviço, o que de facto ocorreu, devido a um ataque de negação de serviço (DoS). O remetente das comunicações ameaçadoras vangloriava-se nas suas mensagens de que seria inútil tentar rastrear de onde estas estavam a ser efetivamente enviadas. Vários estudantes reportaram ter recebido um convite vindo de um perfil designado «Timberlinebombinfo» na página *MySpace*, solicitando colaboração na divulgação das ameaças, sob pena de verem os seus nomes vinculados como autores.

O pedido judicial partiu do agente especial Norman Sanders[84], na sequência de sucessivas evacuações da escola, dadas as diversas ameaças, que originaram interrupções das atividades letivas por vários dias. No requerimento, indicava que havia causa provável para usar o CIPAV na conta «Timberlinebombinfo» do *MySpace*, bem como nos endereços de *e-mail* do autor das ameaças. Este programa permitiria, pela utilização de comandos de computador da *Internet*, solicitar respostas, enviando mensagens ao nível da rede e/ou informações de registo pela *Internet* a um computador pertencente ao FBI[85].

Sanders esclareceu que as funcionalidades do *software* malicioso seriam, entre outras, a obtenção do verdadeiro endereço IP atribuído ao computador e/ou endereço MAC (*Media Access Control*), lista de programas em execução, sistema operativo (tipo, versão e número de série), nome do utilizador conectado no momento e também o último *website* que o computador de destino visitara[86].

Deferida a medida, o FBI instalou o CIPAV na página do *MySpace* e este foi transferido para o computador de destino, no momento em que o utilizador acedeu ao seu

[82]No ano de 2011, a Electronic Frontier Foundation, sob a proteção do Freedom of Information Act, pediu informações acerca do CIPAV que foram disponibilizadas pelo FBI e podem ser consultadas em «New FBI Documents Provide Details on Government's Surveillance Spyware» (29 de abril de 2011), no *site* da fundação: https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav (consultado em 02/06/2021)
[83]GERCKE, Marco. *Understanding Cybercrime: A Guide for Developing Countries*. Genebra: ITU. 2009, p. 204 — 206
[84]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 326
[85]OWSLEY, Brian L. «Beware of Government Agents Bearing Trojan Horses». *Akron Law Review*, Vol. 48, Tomo 2. 2015, p. 324 — 328
[86]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 326

perfil. Foi a primeira oportunidade em que se registou o uso de uma NIT (*network investigative technique*)[87,88].

O código malicioso permitiu a obtenção de um CD com os dados e a efetivação da prisão de um aluno daquela escola, naquela altura contando com apenas 15 anos de idade.

Em retrospetiva, é compreensível que o juiz não dispusesse da informação de que o computador de destino do mandado de busca e apreensão dos dados estivesse territorialmente localizado nos EUA, o que poderia ter levantado questões relacionadas com as normas de competência e conflitos com países terceiros que pudessem sentir-se atingidos na sua soberania.

A propósito deste acontecimento, o mandado firmou-se no art.º 41.º(b)(3) do *Federal Rules of Criminal Procedure*[89], que autoriza um juiz a emitir mandados a serem efetivados dentro ou fora dos limites territoriais do distrito, quando no âmbito de uma investigação sobre terrorismo.

O órgão de investigação federal norte-americano continuou a fazer uso de *software* malicioso nas suas investigações ao longo dos anos seguintes, como exemplifica uma decisão datada de 22 de abril do ano de 2013, proferida pelo juiz Stephen Smith, em Houston, no estado norte-americano do Texas[90]. Tal decisão judicial veio como resposta a um pedido decorrente de uma investigação policial chefiada pelo FBI, com a qual tentava apurar crimes contra a lei de fraude bancária federal, furto de identidade e acesso ilegítimo a sistema informático.

Os factos que motivaram o início das investigações relacionavam-se com um cidadão chamado John Doe, que, na data dos acontecimentos, residia no estado do Texas. Este tinha sido vítima de um crime de acesso ilegítimo à sua conta de *e-mail*, a partir de um endereço IP localizado fora dos EUA, que permitiu ao criminoso o subsequente ingresso na conta bancária de John Doe. Após confirmar a existência de saldo disponível na conta da vítima, o infrator criou um novo endereço de *e-mail* semelhante ao usado naquela altura por John Doe (divergindo apenas uma letra), e enviou mensagem ao banco solicitando que fosse

[87]THOMPSON II, Richard M. *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure*. 8 de setembro de 2016, p. 2 – 3. Obtido de Congressional Research Service: https://fas.org/sgp/crs/misc/R44547.pdf

[88]N. do A. —No mesmo sentido, vd. POULSEN, Kevin. «FBI's PC spy malware tactics revealed». Obtido de https://www.wired.co.uk/ (consultado em 03/05/2021)

[89]A legislação citada pode ser visualizada em: https://www.law.cornell.edu/rules/frcrmp/rule_41 (Federal Rules of Criminal Procedure. «Rule 41. Search and Seizure». Legal Information Institute, Cornell Law School; consultada em 05/02/2021)

[90]A decisão está disponível em: https://www.govinfo.gov/content/pkg/USCOURTS-txsd-4_13-mj-00234/pdf/USCOURTS-txsd-4_13-mj-00234-0.pdf (U.S. Government Info. CIVIL ACTION NO. 4:13-CV-3291; consultada em 06/06/2021)

transferida uma quantia em dinheiro para uma conta de uma instituição financeira situada no estrangeiro.

Ignorando por completo a real identidade e o paradeiro do transgressor, o FBI elaborou um requerimento de busca e apreensão dirigido ao magistrado judicial, petição na qual transparecia a intenção de instalar de modo sub-reptício um *malware* no sistema informático do visado, com a finalidade de extrair dados constantes do computador de destino. Os investigadores pretendiam aceder a informações já constantes no interior do sistema informático alvo, como, por exemplo, registos de endereços de IP usados, registos de atividade na Internet, incluindo *logs* de *firewall*, *caches*, histórico do navegador e *cookies*, páginas da *Web* marcadas como favoritas, termos de pesquisa que o utilizador tivesse inserido em qualquer motor de pesquisa da *Internet* e registos de endereços da *Web* digitados pelo utilizador. Pretendiam também aceder a registos que evidenciassem o uso de endereços de IP para comunicar com os servidores de *e-mail* do banco onde a vítima mantinha valores, bem como a evidências de quem usara, detivera ou controlara o computador alvo da infeção por código malicioso, no momento em que as informações descritas foram geradas, editadas ou excluídas, como registos de entradas, arquivos de configuração, nomes de utilizador e senhas guardadas, documentos, histórico de navegação, perfis de utilizador, conteúdo de *e-mail*, contactos de *e-mail*, aplicações de mensagens instantâneas, *logs* de mensagens, fotografias e correspondência. Os investigadores procuravam ainda a evidência da presença de *software* que permitiria o eventual controlo do computador alvo da investigação por terceiros, bem como a evidência dos horários em que o computador infetado por código malicioso teria sido usado e registos de aplicações executadas, constantes do disco rígido, presentes na memória RAM (*Random Access Memory*) ou noutras formas de armazenamento.

Além das informações já citadas, os agentes do FBI pretendiam obter dados gerados após a intrusão do *malware* no computador de destino, incluindo dados externos ao sistema informático alvo da busca. Estes seriam recolhidos durante um período de monitorização de 30 dias, contando com fotografias obtidas por ativação da câmara presente no computador, necessárias para identificar os utilizadores do computador-alvo; lançamentos contabilísticos que refletiriam a identificação de novas vítimas de fraude, e ainda informações sobre a localização física e geográfica do sistema informático alvo da busca, enviando aos agentes do FBI coordenadas de latitude e longitude que o *malware* induziria o computador infetado a calcular, enviando todos estes dados aos investigadores no Texas.

O requerimento policial baseava-se no art.º 41.º do *Federal Rules of Criminal Procedure*[91], porém o tribunal não concedeu a ordem, uma vez que entendeu que não se verificavam os requisitos territoriais impostos pelo art.º 41.º nem os requisitos de particularidade ou os requisitos para vigilância por câmara impostos pela Quarta Emenda à Constituição.

No que concerne aos requisitos territoriais, os agentes do FBI admitiram que a localização do computador alvo da busca e apreensão era ignorada desde a interposição do requerimento, fundamentando a petição com o art.º 41.º(b)(1), norma que estabelece a competência do juiz para expedir mandados de busca e apreensão de uma propriedade localizada no distrito. Outrossim, o magistrado judicial compreendeu que os agentes pretendiam uma busca pelo computador utilizado pelo infrator e também pelos dados armazenados ou gerados por este mesmo computador, sendo que ambas seriam efetivadas num local físico fora do distrito onde a decisão foi emitida. A argumentação invocada no requerimento conduzia à conclusão de que os agentes estariam autorizados a realizar buscas e apreensões de dados em qualquer lugar do Planeta, desde que estes dados fossem analisados no interior do distrito. Após escrutinar cada um dos cinco fatores que estabelecem a competência territorial de um magistrado judicial para expedir mandados de busca e apreensão em determinado distrito com base no art.º 41.º, o magistrado judicial concluiu que não havia base legal para deferir a medida num computador cuja localização era desconhecida.

O juiz Stephen Smith considerou também que não estaria preenchido o requisito da particularidade[92] imposto pela Quarta Emenda à Constituição, que, em conjunto com a causa provável, são as garantias de envergadura constitucional contra buscas genéricas que protegem os cidadãos norte-americanos[93]. Este magistrado entendeu que a petição não esclarecia como o computador-alvo seria encontrado, afirmando que, ao recorrer ao endereço IP com o fim de proceder à instalação do *malware* no dispositivo-alvo, o Governo arriscava a infeção do computador de um indivíduo inocente, dada a prática comum entre

[91]A legislação citada pode ser visualizada em: https://www.law.cornell.edu/rules/frcrmp/rule_41 (Federal Rules of Criminal Procedure. «Rule 41. Search and Seizure». Legal Information Institute, Cornell Law School; consultada em 05/02/2021)

[92]Juliana Campos ensina que a particularidade é a obrigação do requerente em identificar o alvo do mandado [CAMPOS, Juliana. *O Malware como Meio de Obtenção da Prova em Processo Penal*. Coimbra: Edições Almedina. 2021; p. 56 (Versão eletrónica)]

[93]Considerando que, por diversas vezes, o motivo do recurso ao *malware* é precisamente identificar o autor de atos ilícitos, o judiciário havia já admitido a possibilidade de conceder mandados «antecipatórios» [GUTHEIL, Mirja et al. «Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices: Study for the LIBE Committee.» *Policy Department for Citizens' Rights and Constitutional Affairs.* 2017, p. 122 — 123 (consultado pela última vez em 2/6/2021)]

cibercriminosos de disfarçar os seus endereços de IP para se tornarem anónimos quando ligados à Internet. O mesmo poderia verificar-se caso o endereço de *e-mail* fosse utilizado para proceder à infeção, não havendo como precisar que apenas o culpado tivesse acesso à conta de *e-mail* usada.

Por fim, o juiz concluiu que não haveria diferença entre monitorização por fotos e vigilância por vídeo, argumentando que tal prática constituía um método extremamente intrusivo e potencialmente indiscriminado. Isto porque os agentes teriam acesso à câmara instalada no computador, podendo registar fotografias durante todo o período de vigência da ordem.

Afirmou que, para a sua implementação, seria necessária a observância de uma declaração de que outros métodos de investigação haviam sido tentados e falhados, ou que seria improvável que qualquer outro método tivesse sucesso, caso fosse colocado em prática, ou ainda que o mesmo método se revelasse muito perigoso, demonstrando, neste ponto, uma verdadeira dimensão de subsidiariedade a que estaria submetido o deferimento deste aspeto particular.

Ressaltando que o *software* não apresentava garantias de que apenas os dados mínimos necessários e indispensáveis para a investigação seriam coletados, o magistrado judicial afirmou que um pedido semelhante poderia vir a ser deferido no futuro, caso os agentes da polícia conseguissem trazer respostas satisfatórias para as preocupações expostas na decisão.

A repercussão gerada pelo indeferimento da medida solicitada pelo FBI chegou ao Congresso norte-americano por iniciativa da Suprema Corte dos Estados Unidos, a 28 de abril de 2016[94], e, por sua vez, o Poder Legislativo aprovou, no dia 16 de dezembro de 2016, uma modificação, acrescentando o art.º 41.º(b)(6) ao *Federal Rules of Criminal Procedures*[95]. Essencialmente, um magistrado passou a ter competência para, independentemente de conhecer a localização dos alvos, determinar o acesso remoto para pesquisar, copiar ou apreender informações constantes de sistemas informáticos dentro ou fora do distrito onde exerce jurisdição, desde que a localização do dispositivo tenha sido ocultada por meios tecnológicos, ou ainda quando esteja em curso uma investigação de crime

[94]THOMPSON II, Richard M. *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure*. 8 de setembro de 2016, p. 4 – 5. Obtido de Congressional Research Service: https://fas.org/sgp/crs/misc/R44547.pdf

[95]CAMPOS, Juliana. *O Malware como Meio de Obtenção da Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 55 (Versão eletrónica)

informático em que o atacante tenha causado danos em sistemas informáticos concomitantemente em cinco ou mais distritos, o que é comum, no caso das *botnets*[96].

2.2. A admissibilidade do *malware* em Espanha

Mesmo após a ratificação em Espanha da Convenção sobre o Cibercrime, que decorreu em Budapeste, no ano de 2001, em que já se apresentava a necessidade de regulamentar o uso de *malware*[97], o legislador daquela nação absteve-se de regulamentar a utilização dos avanços tecnológicos nos trabalhos desenvolvidos relativamente à elucidação de crimes[98].

Esta situação colocou os juízes diante da difícil escolha entre a impunidade de factos delituosos ou o deferimento de medidas investigativas para recolha de provas sem a estrita e clara previsão legal, o que, efetivamente, reclamava uma alteração processual para equacionar o conflito[99].

No ano 2011, o conselho de ministros espanhol elaborou e enviou ao Poder Legislativo um projeto de mudança na lei processual penal, onde constava a adaptação das normas relacionadas com a investigação criminal aos ditames da realidade proporcionada pelas inovações técnicas trazidas pela ciência. Este projeto procurava dar resposta às exigências que se apresentavam naquela época. Não obstante, o mesmo ainda não contemplava a previsão do uso de *malware*, e o parlamento não foi capaz de concluir a aprovação daquela proposta[100].

Em 2012, na sequência de estudos elaborados por uma comissão, o ministro da justiça espanhola apresentou um novo projeto de alteração legislativa, denominado «Projeto

[96]ADAMS, Devin M. «The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, "Particularly Speaking"». Obtido de *University of Richmond Law Review*, Vol. 51: http://lawreview.richmond.edu/files/2017/03/Adams-513.pdf. 2017, p. 727 (consultado pela última vez em 02/05/2021)

[97]ZARAGOZA TEJADA, Javier Ignacio. «El registro remoto de equipos informáticos». *Investigación Tecnológica y Derechos Fundamentales: Comentarios a las modificaciones introducidas por la Ley 13/2015*. Navarra: Editorial Aranzadi. 2017, p. 474 (Versão eletrónica)

[98]ORTIZ PRADILLO, Juan Carlos. (2017). «Desafíos legales de las diligencias de investigación tecnológica». AA.VV. *El Proceso Penal – Cuestiones Fundamentales.* Valência: Tirant to Blanch. 2017, p. 305 — 306

[99]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 332

[100]VACIAGO, Giuseppe e RAMALHO, David Silva. «Online searches and online surveillance – the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings.» *Digital Evidence and Electronic Signature Law Review*. 2016, p. 93

Gallardón», que já previa a intrusão remota, por meio de *software*, num sistema informático para a recolha de dados, que também não foi objeto de aprovação parlamentar[101,102].

Apenas a 5 de outubro do ano de 2015 foi sancionada a lei 13/2015, que trouxe profundas mudanças para a *Ley de Enjuiciamiento Criminal* (LECrim), tendo entrado em vigor no final daquele mesmo ano. Pela primeira vez, o ordenamento jurídico espanhol abarcava uma diversidade de medidas de investigação tecnológica, inserindo inclusive a figura do «registo remoto sobre *equipos* informáticos», nos artigos 588.º *septies* A, B e C[103].

O art.º 588.º, *septies* A, prevê que

> «o juiz de instrução poderá autorizar a utilização de dados de identificação e códigos, assim como a instalação de um *software*, que permitam, de forma remota e telemática, o exame feito em distância e sem o conhecimento do seu titular ou utilizador do conteúdo de um computador, dispositivo eletrónico, sistema informático, instrumento de armazenamento em massa de dados informáticos ou base de dados, sempre que se persiga a investigação de um dos crimes enumerados»[104].

Preveem-se, assim, duas formas pelas quais um investigador poderá ter acesso aos dados armazenados num sistema de processamento ou armazenamento de dados. A primeira forma prende-se com a utilização de dados de identificação e códigos como, por exemplo, no caso de o agente estatal ter as informações de acesso e a palavra-passe de um serviço baseado em *software* disponível na *Internet*, assim como acontece, por exemplo, com os serviços de computação em nuvem[105].

Tais informações poderiam estar disponíveis para os investigadores pela posse física do sistema informático, no qual já estariam armazenadas, ou pelo fornecimento pelas empresas que prestam o serviço, cumprindo uma obrigação legal. A doutrina costuma designar esta hipótese por «registos estendidos», por ocorrer, normalmente, a partir de um registo inicial do sistema informático[106].

---

[101]RAMALHO, David Silva. «O uso de *malware* como meio de obtenção de prova em processo penal». *Revista de Concorrência e Regulação,* Ano IV, n.º 16. Out. — dez. de 2013, p. 222

[102]ZARAGOZA TEJADA, Javier Ignacio. «El registro remoto de equipos informáticos». *Investigación Tecnológica y Derechos Fundamentales: Comentarios a las modificaciones introducidas por la Ley 13/2015*. Navarra: Editorial Aranzadi. 2017, p. 476 (Versão eletrónica)

[103]WINTER, Lorena Bachmaier. «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015». *Boletín del Ministerio de Justicia*, Ano LXXI, n.º 2195. 2017. Obtido de: https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/InstLibraryDoctrinalStudies/1701_Estudio.pdf (consultado pela última vez em 10/07/2021)

[104]N. do A. — Tradução livre do artigo da lei.

[105]DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones.* Madrid: Wolters Kluwer. 2016 (Versão eletrónica)

[106]WINTER, Lorena Bachmaier. (2017). «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015». *Boletín del Ministerio de Justicia*, Ano LXXI, n.º 2195.

A segunda forma prevista de acesso dos investigadores a dados armazenados consiste na instalação de um *software* malicioso que lhes permita obter o conteúdo do sistema informático de modo remoto e telemático, sem o conhecimento do utilizador e sem a necessidade de solicitar informações aos provedores de *Internet*[107], sendo precisamente esta a modalidade de obtenção de prova que condiz com o objeto deste estudo. Tal mecanismo de investigação está sujeito aos princípios estabelecidos no art.º 588.º *bis* a (LECrim), quais sejam: especialidade, idoneidade, excecionalidade, necessidade e proporcionalidade. A letra da lei impede ainda que qualquer servidor público proceda à instalação do *software* malicioso sem a autorização do juiz de instrução, mesmo em caso de urgência[108].

A lei determina que esta autorização concedida pelo juiz de instrução deverá conter: a individualização dos sistemas informáticos, meios informáticos de armazenamento de dados ou quaisquer conteúdos digitais que se pretenda obter com a medida; o alcance preciso da medida, a forma que será utilizada para se proceder ao acesso e à apreensão dos dados ou ficheiros informáticos necessários para a investigação criminal, assim como a especificação do código malicioso com o qual se executará a intrusão e captura dos dados. Deverá ainda incluir os investigadores que serão autorizados para a execução da medida, as providências tomadas para a preservação da integridade dos dados e da cadeia de custódia da prova, bem como a autorização para a realização de cópias dos dados ou supressão dos mesmos.

Cientes de que a medida implica uma elevada ingerência para uma enorme quantidade de informações, além de uma grave extensão de potenciais danos aos direitos humanos, os legisladores estabeleceram um rol *numerus clausus* de delitos especialmente graves que poderiam desencadear o deferimento da medida, o que foi considerado desafortunado por parte da doutrina[109].

No entanto, não foram eleitas apenas classes de tipos penais específicos, como o terrorismo, abarcando também sujeitos passivos, como menores ou pessoas com capacidade judicialmente modificada. Isto implicaria que tivessem sido, eventualmente, abertas as portas para que tais medidas invasivas pudessem ser aplicadas em situações em que se investigam quaisquer crimes de menor gravidade, como, por exemplo, crimes contra a honra,

Obtido de: https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/InstLibraryDoctrinalStudies/1701_Estudio.pdf (consultado em 10/07/2021)

[107]DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones.* Madrid: Wolters Kluwer. 2016 (Versão eletrónica)

[108] Idem

[109]ZARAGOZA TEJADA, Javier Ignacio. «El registro remoto de equipos informáticos». Em *Investigación Tecnológica y Derechos Fundamentales: Comentarios a las modificaciones introducidas por la Ley 13/2015*. Navarra: Editorial Aranzadi. 2017, p. 479 — 482 (Versão eletrónica)

desde que o sujeito passivo fosse uma pessoa menor, o que recomenda prudência aos magistrados na análise de pedidos[110].

Ao fazer referência ao termo «conteúdo», a legislação parece não abranger comunicações em tempo real, como aquelas que ocorrem através de aplicações que criptografam ligações VoIP entre sistemas informáticos conectados com a Internet[111]. Do mesmo modo, não se vislumbra ter sido facultada por lei a ativação de partes do *hardware* do sistema informático, como câmaras e microfone.

Se considerarmos as aplicações que criptografam mensagens escritas, não restam dúvidas de que poderiam ser apreendidas em qualquer momento, durante a vigência da ordem de investigação tecnológica. Isto ocorre porque a interceção de telecomunicações e o registo de conteúdos constituem medidas distintas, e apenas a primeira prevê a possibilidade de captação de dados futuros. Porém, esta posição doutrinária não é unânime[112].

A medida poderá ter duração máxima de um mês, prorrogável por iguais períodos, até o máximo de três meses, nos termos do art.º 558.º *septies* C, devendo ser especificada no pedido do *Ministerio Fiscal* ou da *Policía Judicial* o tempo pretendido para que a investigação tecnológica perdure, de acordo com o teor do art.º 588.º *bis* B[113]. Os prazos deverão ser contados a partir da decisão judicial, salvo acolhimento pelo juiz da instrução de argumentação, no sentido de que tenham ocorrido dificuldades técnicas na instalação do *software*, exemplo que pode ser contado a partir da efetivação da intrusão[114].

2.3. A admissibilidade do *malware* na Alemanha

Desde há muitos anos, os órgãos de controlo na Alemanha já vislumbravam a possibilidade de se infiltrarem em sistemas informáticos através do uso de *malware*, para recolha de dados que pudessem ser usados em investigações criminais. Uma das

[110]GARCIMANTÍN MONTERO, Regina. *Los médios de investigación tecnológicas en el processo penal*. Navarra: Editorial Aranzadi. 2018 (Versão eletrónica)
[111]WINTER, Lorena Bachmaier. «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015». *Boletín del Ministerio de Justicia*, Ano LXXI, n.º 2195. 2017. Obtido de: https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/InstLibraryDoctrinalStudies/1701_Estudio.pdf (consultado em 10/07/2021)
[112]ZARAGOZA TEJADA, Javier Ignacio. «El registro remoto de equipos informáticos». *Investigación Tecnológica y Derechos Fundamentales: Comentarios a las modificaciones introducidas por la Ley 13/2015*. Navarra: Editorial Aranzadi. 2017, p. 477 (Versão eletrónica)
[113]CAMPOS, Juliana. *O Malware como Meio de Obtenção da Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 58 (Versão eletrónica)
[114]N. do A. — É importante observar que houve um comedimento do legislador no que tange aos prazos, quando comparados com o das intercetações telefónicas, que podem ter duração de até dezoito meses nos termos do artigo 588.º *ter* g.

demonstrações é a decisão do Tribunal Federal de Justiça (*Bundesgerichtshof* — BGH), datada de 21 de fevereiro de 2006[115].

Neste julgamento, foi concedida pela corte judicial uma «busca *on-line*», informando que as autoridades investigadoras estariam autorizadas a inserir um *software* malicioso no sistema informático utilizado pelo acusado com o intuito de copiar dados armazenados, amparando-se a admissibilidade da busca pela comparação com uma pesquisa clássica por métodos clandestinos.

Considerou-se que o Código de Processo Penal (StPO), apesar de não conter disposição expressa que autorizasse a prática, poderia ser interpretado de modo a conceber o uso de *malware* como algo semelhante a uma diligência investigativa, na qual o proprietário ou possuidor visado pela medida estivesse ausente durante a execução.

Ressaltou que em sociedades nas quais as tecnologias da informação e comunicação desempenham um amplo papel na vida dos membros da comunidade, o ordenamento jurídico estaria fundamentalmente aberto para acolher as evoluções apresentadas pela ciência forense.

A decisão deixou igualmente expresso que não estariam em perigo direitos fundamentais como a inviolabilidade do domicílio e que não haveria processo de telecomunicação durante a recolha dos dados via *Internet* a atrair requisitos específicos da conceção de uma intercetação de telecomunicações.

Ainda assim, mesmo dentro da jurisprudência alemã, tal posição não se revelou pacífica, tendo a divergência sido consubstanciada, poucos meses mais tarde, no julgamento de um recurso do Ministério Público que investigava um acusado por fundar uma organização terrorista[116].

A petição de recurso do *parquet* decorreu do indeferimento de um juiz de instrução a requerimento para efetuar uma «busca *on-line* secreta», por meio da introdução de um *software* malicioso no computador do acusado, capaz de transmitir os dados armazenados aos investigadores.

Ao confirmar a posição do juiz de instrução, o tribunal sustentou, em suma, que a «busca *on-line*» não poderia ser equiparada a uma busca física, caracterizada pelo facto de

[115]Decisão do BGH de 21/2/2006 — 3BGs 31/06, disponível em BeckRS 2006, 18459: https://beck-online.beck.de/Dokument?vpath=bibdata%5Cents%5Cbeckrs%5C2006%5Ccont%5Cbeckrs.2006.18459.htm&einzelDokumentenKauf=True (consultado pela última vez em 15/06/2021)

[116]Despacho BGH de 31/1/2007 – StB 18/06, disponível em BeckRS 2007, 1978: https://beck-online.beck.de/Dokument?vpath=bibdata%5Cents%5Cbeckrs%5C2007%5Ccont%5Cbeckrs.2007.01978.htm&einzelDokumentenKauf=True (consultado pela última vez em 15/06/2021)

os investigadores se encontrarem pessoalmente no local da busca, dando conhecimento da investigação ao visado. Salientou que o conhecimento de uma busca seria um requisito formal imposto pelo ordenamento jurídico, não podendo ser omitido do suspeito por interesses táticos, e não se prendendo com disponibilidade dos investigadores.

O tribunal afirmou que as disposições do código de processo penal que tratam da «busca» ou «pesquisa» são obrigatórias para a sua licitude, não sendo possível combinar elementos de autorização constantes da legislação para criar uma nova medida de investigação tecnicamente possível. Expressou ainda que um meio técnico insidioso somente poderia ter lugar se nenhum outro meio de investigação estivesse disponível e se, cumulativamente, não interferisse com a área central inviolável da vida privada.

Não haveria, portanto, no Código de Processo Penal (StPO) base legal para deferir a medida.

Com efeito, a decisão que se tornou um divisor de águas na história alemã acerca do uso de *malware* como meio oculto de obtenção de provas em ambiente digital foi exarada pelo Tribunal Constitucional Federal Alemão (BVerfG), no dia 27 de fevereiro de 2008[117], com a decisão acerca da constitucionalidade do §5.2. (11) da lei sobre a proteção da Constituição da Renânia do Norte-Vestefália, datada de 20 de dezembro do 2006[118].

Esta foi a primeira normativa da Alemanha a conceder expressamente poderes para que um órgão investigativo (Autoridade de Proteção da Constituição) acedesse, em sigilo, aos sistemas de tecnologia da informação com a utilização de *software* malicioso, ou seja, a lei pretendia autorizar o uso de «pesquisas *on-line*», tendo em consideração as dificuldades impostas numa investigação quando os suspeitos utilizam sistemas informáticos e a *Internet* para efetuarem comunicações criptografadas, com o intuito de planear e executar delitos.

O tribunal considerou que o uso das tecnologias da informação e comunicação se tornou central no desenvolvimento pessoal dos cidadãos e que a norma colocada sob avaliação constitucional estaria a violar o direito geral à personalidade, na medida em que o uso destes meios técnicos para infiltração no sistema informático poderia conceder um amplo conhecimento sobre a personalidade do utilizador.

[117] *Judgment of 27 February 2008 — 1 BvR 370/07*. Obtido de Bundesverfassungsgericht: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html (consultado em 20/07/2021)

[118] A legislação citada pode ser visualizada em https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl108s3083.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl108s3083.pdf%27%5D__1630248466439 (consultada em 20/07/2021)

Tal violação ultrapassava a vertente de proteção do direito à autodeterminação informativa, e levou a corte a desvelar o direito fundamental à confidencialidade e integridade dos sistemas informáticos.

Além disso, estabeleceu que uma infiltração secreta num sistema informático somente é admissível quando factos concretos indicam que um crime põe em perigo bens jurídicos extremamente relevantes, como, por exemplo, os fundamentos ou a existência do Estado, ou, ainda, o corpo, a vida e a liberdade de uma pessoa, estando, em regra geral, dependente de autorização judicial.

Sublinhou que a norma atacada não obedecia aos critérios de clareza e especificidade, impedindo os seus destinatários de reconhecerem a situação jurídica e de se prepararem para as medidas que dela pudessem decorrer, afetando indiretamente a liberdade dos cidadãos, que poderiam deixar de se comunicar livremente, com receio de se encontrarem sob vigilância.

Concluiu afirmando que não tinham sido adotadas precauções legais para evitar a invasão da área central absolutamente livre de ingerência estatal, como sensações, sentimentos, reflexões, visões e experiências de natureza estritamente pessoal e que, deste modo, as disposições atacadas eram nulas e sem efeito.

Partindo de pressupostos estabelecidos pelo Tribunal Constitucional Federal Alemão (BVerfG) para a aprovação de uma legislação prevendo o uso de *malware* na obtenção de provas criminais, no dia 25 de dezembro de 2008, foi aprovada a Lei de Defesa Contra os Perigos do Terrorismo Internacional através da Polícia Judiciária Federal (*Bundeskriminalamt – BKA*)[119,120].

Entre os poderes conferidos à Polícia Judiciária Federal pelo §49k[121] da dita Lei, com o intuito de combater crimes considerados graves — especialmente o terrorismo —, estão as providências de infiltrações clandestinas em sistemas informáticos para recolha de dados («buscas *on-line*»), porém com atuação exclusiva a título preventivo[122].

[119]A legislação citada pode ser consultada em: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl108s3083.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl108s3083.pdf%27%5D__1630331134197 (consultada em 06/05/2021)

[120]O preceito citado sofreu alteração legislativa devidamente publicada em 01/06/2017 e disponível para consulta em https://www.bundesgerichtshof.de/DE/Bibliothek/GesMat/WP18/B/BKAG_Neustruktur.html (consultada em 06/05/2021)

[121]N. do A. — Note-se que este artigo é correspondente ao 20k da lei antes da reestruturação legislativa publicada em 01/06/2017.

[122]ROGALL, Klaus. «A nova regulamentação da vigilância das telecomunicações na Alemanha». AA.VV. *2.º Congresso de Investigação Criminal.* Coimbra: Almedina. 2010, p. 120 — 121

Os bens jurídicos eleitos pelo legislador alemão que justificam a providência de intrusão nos moldes acima referidos são o corpo, a vida e a liberdade de uma pessoa ou a ameaça que afete os fundamentos e a existência do governo federal ou de um Estado.

Os riscos que a diretiva pretende obliterar devem ser concretos e previsíveis, pelo que a sua aplicação só é admissível nos casos em que seja muito difícil ou impossível obter os dados de outra forma.

Garante-se, segundo o estado da técnica, que apenas serão realizadas as alterações mínimas indispensáveis no sistema informático do investigado, sendo revertidas no término do prazo para execução da intervenção, e que os dados serão protegidos de alterações, exclusões e acessos não autorizados.

No que tange aos destinatários, só o investigado por um dos crimes constantes do §17 e §18 da Lei da Polícia Federal (*Bundespolizeigesetz*) poderá figurar como alvo da intrusão informática. O pedido de autorização dirigido ao juiz para implementar o *software* espião deve: conter a indicação do indivíduo visado, se possível evidenciando o seu nome e a sua morada, descrever pormenorizadamente o sistema informático com o qual serão recolhidos os dados, indicar a duração e a finalidade do meio, fundamentar a necessidade de uso do *malware*, apontando os factos que ensejam o pedido.

Devem ser adotadas medidas técnicas para evitar a recolha de dados relacionados com a área nuclear essencial da vida privada, sendo inadmissível qualquer infiltração por *software* que perspetive unicamente a recolha de dados relacionados com a dita área. De qualquer modo, todos os dados devem ser submetidos ao juiz, que deverá decidir quais são elegíveis para usabilidade ou exclusão.

Não obstante o facto de haver uma lei que legitimava a Polícia Federal a utilizar *malware* em determinadas circunstâncias, no dia 8 de outubro de 2011, uma comunidade de *hackers* autointitulada *Chaos Computer Club* (CCC) anunciou aos órgãos de imprensa que as polícias de diversos estados alemães estariam a fazer uso de um código malicioso para o desempenho das suas atribuições, que veio, posteriormente, a ser denominado de *Bundestrojaner* ou *Staatstrojaner*[123,124].

O *malware* adquirido pelos órgãos de controlo possibilitou a obtenção de informações acerca de toda a atividade desenvolvida pelo investigado, como, por exemplo, a interceção de chamadas VoIP (chamadas de voz sobre IP fornecidas por aplicações como o *Skype* ou o

[123]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 329
[124]WEBER, Rolph e HEINRICH, Ulrike I. *Anonymization.* Londres: Springer. 2012, p. 60

WhatsApp), registo de teclas premidas, introdução de dados na memória do dispositivo e ativação remota de partes do *hardware* como câmaras e microfones[125].

Ciente de que a legislação que autorizava a infiltração de *software* malicioso existente até então apenas assegurava a prevenção de riscos[126], o parlamento daquela nação (*Bundestag*) fez publicar, no dia 23 de agosto de 2017, importantes alterações que autorizavam o uso de *malware* no Código de Processo Penal (StPO), com entrada em vigor logo no dia seguinte[127].

Assim, hodiernamente, o §100a, n.º 1 (StPO),[128] traz sobre a epígrafe de vigilância de telecomunicações, além das já conhecidas intercetações telefónicas, a possibilidade de «vigilância na fonte» (*Quellen-TKÜ*)[129], em que o *malware* inserido no sistema informático do visado funcionaria como um «ouvinte» que acede à comunicação antes de ser criptografada, ou seja, antes de ser enviada, ou depois de ser desencriptada, i.e., recebida. Este método oculto de investigação foi criado para possibilitar a escuta de conversas telefónicas realizadas através de aplicações como as supramencionadas, que possibilitam ligações VoIP[130] e que, a cada dia mais, substituem as clássicas ligações telefónicas.

Por outro lado, o legislador previu, no §100b (StPO), o uso do *software* de vigilância nas chamadas «buscas *on-line*»[131], desta feita para aceder a dados armazenados ou produzidos em tempo real, tendo conteúdo de comunicações atuais ou anteriores, constantes das memórias RAM e ROM (*read-only memory*) do sistema informático, como *e-mail*s,

[125]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 329

[126]SOINÉ, Michael. «Die strafprozessuale Online-Durchsuchung». *NStZ,* n.º 9. 2018, p. 497. Disponível em: https://beck-online.beck.de/ (consultado pela última vez em 15/06/2021)

[127]KOCHHEIM, Dieter. «Onlinedurchsuchung und Quellen-TKÜ in der Strafprozessordnung – Neuordnung der tiefen technischen Eingriffsmaßnahmen in der StPO seit dem 24.8.2017». *KriPoz, Ed. 2*. 2018, p. 60. disponível em https://kripoz.de/2018/03/01/onlinedurchsuchung-und-quellen-tkue-in-der-strafprozessordnung-neuordnung-der-tiefen-technischen-eingriffsmassnahmen-in-der-stpo-seit-dem-24-8-2017/ (consultado pela última vez em 15/06/2021)

[128]A legislação citada pode ser consultada em: https://www.gesetze-im-Internet.de/stpo/__100a.html (consultado pela última vez em 15/06/2021)

[129]KOCHHEIM, Dieter. «Onlinedurchsuchung und Quellen-TKÜ in der Strafprozessordnung – Neuordnung der tiefen technischen Eingriffsmaßnahmen in der StPO seit dem 24.8.2017». *KriPoz,* Ed. 2. 2018, p. 61. Disponível em https://kripoz.de/2018/03/01/onlinedurchsuchung-und-quellen-tkue-in-der-strafprozessordnung-neuordnung-der-tiefen-technischen-eingriffsmassnahmen-in-der-stpo-seit-dem-24-8-2017/ (consultado pela última vez em 15/06/2021)

[130]Da mesma maneira, outras aplicações como o WhatsApp disponibilizam trocas de mensagens e ligações VoIP usando criptografia, uma técnica para garantir o sigilo das informações, conhecido como «*end-to-end encryption*» ou «encriptação ponto-a-ponto», em que as chaves públicas e privadas para desencriptar a informação estão apenas nos sistemas informáticos dos comunicantes, de modo que o servidor por onde estas mensagens navegam não possuem acesso ao seu conteúdo, conforme TEIXEIRA, Tarcisio et al. «Criptografia e segurança de redes: considerações gerais e a sua inserção no WhatsApp». Belo Horizonte: *Revista da Faculdade de Direito da Universidade Federal de Minas Gerais,* n.º 71. Julho — dezembro de 2017, p. 624.

[131]SOINÉ, Michael. «Die strafprozessuale Online-Durchsuchung». *NStZ,* n.º 9. 2018, p. 497. Disponível em: https://beck-online.beck.de/ (consultado pela última vez em 15/06/2021)

mensagens SMS e *WhatsApp*, arquivos de fotos, contactos de aplicações sociais e dados constantes em nuvem, acessíveis a partir do sistema informático invadido[132].

Assim, os crimes passíveis de serem investigados no âmbito da «vigilância na fonte» encontram-se enumerados numa extensa lista constante do §100a, n.º 2 (StPO), e os crimes passíveis de serem investigados por uma «busca *on-line*» constantes de uma relação *numerus clausus* e elencados numa lista igualmente longa, presente no §100b, n. º 2 (StPO).

Seguindo as indicações elaboradas na decisão do Tribunal Constitucional Federal acima mencionada, apenas poderiam ser atingidos o investigado ou quem presumivelmente receba e transmita mensagens para o mesmo, sempre que se trate de «vigilância na fonte». Já num cenário de «buscas *on-line*», além do investigado, poderão estar sujeitos à infiltração dos respetivos sistemas de tecnologia da informação terceiros, sempre que estejam a ser utilizados pelo visado.

Ficou também determinado, no §100a, n.º 5 (StPO), que apenas serão realizadas as alterações mínimas indispensáveis para a recolha de dados relacionados com as telecomunicações, sendo revertidas no término do prazo para execução da intervenção.

Ainda foi estabelecido, pela norma que regulamenta a «vigilância na fonte», que cada vez que um *software* espião for utilizado, será gerado um relatório a indicar os meios técnicos usados e o tempo da sua utilização, as informações sobre as características do sistema de tecnologia da informação e as mudanças nele realizadas, trazendo informações que permitam apurar os dados recolhidos e a unidade investigativa que encetou a medida.

Aplicável a ambos os cenários de investigação oculta, o §100d (StPO)[133] determina que a medida será inadmissível caso obtenha informações relacionadas com o núcleo fundamental da vida privada. O recurso às mesmas será necessariamente vedado, caso qualquer informação desta estirpe seja obtida inadvertidamente.

O §100e, n. º 1[134], indica que a duração máxima da medida de «vigilância na fonte» será de três meses, prorrogável uma vez por igual período, no caso de permanecerem presentes os seus requisitos. A «vigilância na fonte» poderá ser determinada pelo membro do Ministério Público em caso de urgência, desde que confirmada pelo juiz no prazo de três dias. Concede-se um prazo mais apertado para a «busca *on-line*», com uma duração máxima

[132]SOINÉ, Michael. «Die strafprozessuale Online-Durchsuchung». *NStZ*, n.º 9. 2018, p. 502. Disponível em: https://beck-online.beck.de/ (consultado pela última vez em 15/06/2021)
[133]A legislação citada pode ser visualizada em: https://www.gesetze-im-Internet.de/stpo/__100d.html
[134]Idem

de um mês, prorrogável uma única vez por igual período, caso os requisitos se mantenham presentes.

3. A LIMITAÇÃO DA ATIVIDADE PROBATÓRIA EM PROCESSO PENAL IMPOSTA PELOS DIREITOS FUNDAMENTAIS

3.1. A legalidade como condição procedimental em investigação criminal

Acerca do tema proposto para análise, constata-se que a finalidade última de se recorrer ao *software* malicioso durante a investigação de crimes é a recolha e análise de fontes de prova eletrónico-digitais.

Tendo em consideração os ensinamentos de Benjamim Silva Rodrigues, pode-se conceituar a prova digital como «informação com valor probatório armazenada ou transmitida em formato digital»[135], ou, ainda, segundo Eoghan Casey, como

> «qualquer dado armazenado ou transmitido usando um computador que apoia ou refuta uma teoria de como um crime ocorreu ou que abordem elementos críticos do crime, como intenção ou álibi»[136].

Este é um tipo de fonte de prova obtida numa linguagem binária, uma sequência de números, e, consequentemente, imaterial, antes da conversão por um processador de dados, que a transmute para um formato percetível aos sentidos humanos, como, por exemplo, textos, áudios, imagens e vídeos. Caracteriza-se pela efemeridade ou precariedade, fragilidade ou alterabilidade, e volatilidade ou instabilidade[137].

O âmbito da fonte de prova digital é bem mais amplo do que o fenómeno da cibercriminalidade, já que qualquer investigação pode demandar a recolha desta natureza de fonte de prova, ainda que um dispositivo eletrónico-digital não tenha sido utilizado para a execução do delito, conforme o art.º 11.º, n.º 1, al. c) da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro).

É importante ressaltar que qualquer informação é passível de ser digitalizada, podendo ser armazenada e transportada para atender à necessária celeridade que emana do processo penal, e que resulta na adoção de medidas que gerem convicções inabaláveis ao magistrado judicial para suprir esta precisão.

A adoção do uso de *malware* pelo Estado na obtenção de fontes de prova tem o intuito de facultar informações ao processo penal, classificadas, segundo José de Mouraz Lopes,

---

[135]RODRIGUES, Benjamim da Silva. *Da Prova Penal — Tomo II. Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*. Lisboa: Rei dos Livros. 2010, p. 40

[136]CASEY, Eoghan. «Foundations of Digital Forensics». AA.VV. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* — 3.ª ed. Academic Press/Elsevier. 2011, p. 7 (tradução livre do autor)

[137]RODRIGUES, Benjamim da Silva. *Da Prova Penal — Tomo II. Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*. Lisboa: Rei dos Livros. 2010, p. 40

como dados de localização, dados de tráfego, dados de base e de conteúdo[138]. A amálgama destas informações pode ser organizada, catalogada e analisada para conceber um quadro mais completo e sólido do que se consideradas individualmente, o que poderia ser implementado, por exemplo, por intermédio de um sistema de inteligência artificial para detetar intenções opacas de um programador[139].

No que pertence ao objeto desta pesquisa, pode olhar-se para estas técnicas de investigação de crimes a partir de um recrudescimento no uso de métodos ocultos de investigação em sistemas informáticos, verificando um ângulo de relação do processo penal com a fonte de prova eletrónico-digital obtida através de mecanismo extrassensorial[140] e, portanto, impercetível.

Neste cenário, as Cartas Magnas de Estados democráticos estabelecem normas de direitos fundamentais, e os ordenamentos infraconstitucionais reverberam proibições de prova como verdadeiras limitações à descoberta da verdade[141].

O campo processual penal traz em si tensões entre liberdade (finalidade de proteção dos direitos fundamentais) e segurança (finalidade de realização da justiça e descoberta da verdade material)[142], sendo que esta última é vista como a premissa da qual partem os estados liberais, trazendo os riscos impostos ao exercício de direitos fundamentais estabelecidos na Carta Política, em prol do combate eficiente de novas formas de criminalidade internacional organizada, nas suas vertentes de comercialização de estupefacientes, terrorismo e pedofilia.

Nas palavras de Jorge de Figueiredo Dias, «o que está aqui em jogo é nada menos que a conceção básica de todo o processo penal. Um Estado democrático tem, pura e simplesmente, de garantir este equilíbrio... ou resignar-se a perecer»[143].

É essencial que se compreenda que as proibições de provas estão voltadas necessariamente para a proteção dos direitos fundamentais relacionados com a liberdade[144],

[138]LOPES, José Mouraz e CABREIRO, Carlos Antão. «A emergência da prova digital na investigação da criminalidade informática». *Sub judice – Justiça e Sociedade, n.º 35*. Abr. — jun. de 2006, p.74
[139]RODRIGUES, Anabela Miranda. *Inteligência Artificial no Direito Penal*. Edições Almedina. 2020, p. 60 (Versão eletrónica, acessível em: https://ebooks.almedina.net/books/9789724089676)
[140]BRITO, Beatriz Seabra de. *Novas Tecnologias e Legalidade da Prova No Processo Penal.* Coimbra: Almedina. 2018, p. 65
[141]CORREIA, João Conde. «A distinção entre prova proibida por violação dos direitos fundamentais e prova nula numa perspectiva essencialmente jurisprudencial». *Revista do CEJ*, n.º 4. 2006, p. 202
[142]ANTUNES, Maria João. *Direito Processual Penal — 2.ª ed.* Coimbra: Almedina. 2018, p. 12 (Versão eletrónica)
[143]Dias, Jorge de Figueiredo. «O Processo Penal Português: problemas e prospectivas». AA.VV. *Que futuro para o Direito Processual Penal? Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português.* Coimbra: Coimbra Editora. 2009, p. 809
[144]MENDES, Paulo de Sousa. *Lições de Direito Processual Penal.* Coimbra: Almedina. 2013, p. 169

que se apresentam como fruto das técnicas e instituições de segurança manobradas pelo Estado.

Desde logo, o princípio da legalidade, e, por seu consectário natural, a reserva de lei compõem garantias fundamentais que assistem e dizem respeito a todos os membros da coletividade e impedem, de um modo pleno, o recurso a *malware* que não esteja claramente tipificado.

Tal ocorrerá com maior justificação por apresentar uma natureza oculta, observando-se os riscos de arbitrariedade necessariamente agravados, pois que já se configurará de plano a compressão do gozo e usufruto dos direitos que o art.º 18.º da Constituição da República Portuguesa (CRP) e art.º 5.º da Constituição da República Federativa do Brasil de 1988 (CRFB/88) quiseram colocar sob a égide legislativa.

É crucial observar que, de todas as vezes que se venha a adstringir os direitos fundamentais, não advirá somente por este motivo um vácuo, pois será preenchido por interesses e expectativas geradas sobre a investigação criminal.

Quando se avalia a implementação do recurso ao *software* malicioso em sede legislativa, encontra-se uma atividade de regulamentação vinculada, que deverá dispor de um «caráter geral e abstrato», sem «efeitos retroactivos», limitada a resguardar outros direitos e interesses de envergadura exclusivamente constitucional[145]. Uma vez no universo adjetivo penal, tal lei deve ser apresentada com características de clareza, conteúdo determinado e com densidade tal que proporcione a almejada segurança jurídica aos destinatários, sem jamais se deixar consagrar uma norma processual penal em branco.

Assim, os órgãos de controlo, durante a busca de elementos da materialidade e autoria de um crime, estão impedidos de modificar ou criar meios mistos de obtenção de fonte de prova eletrónico-digital, em benefício de um «princípio de lealdade do Estado»[146].

Pelas lições de Manuel da Costa Andrade[147], é possível enumerar os requisitos que a lei precisa de demonstrar sempre que pretenda instituir um método oculto de investigação: a presença de um catálogo de crimes, o grau de suspeita, a subsidiariedade, a autorização por autoridade competente e o acesso à informação pelo visado, após o fim da medida.

[145]ANDRADE, José Carlos Vieira de. *Os Direitos Fundamentais na Constituição Portuguesa de 1976* (6.ª ed.) Coimbra: Edições Almedina. 2019, p. 278 — 279

[146]BRITO, Beatriz Seabra de. *Novas Tecnologias e Legalidade da Prova No Processo Penal.* Coimbra: Almedina. 2018, p. 51

[147]ANDRADE, Manuel da Costa. «Métodos Ocultos de Investigação (Plädoyer para uma teoria geral)». AA.VV. *Que futuro para o Direito Processual Penal? Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*. Coimbra: Coimbra Editora. 2009, p. 545

Sob a epígrafe da legalidade da prova, apresenta-se o art.º 125.º do Código de Processo Penal Português (CPP), que, numa leitura superficial, poderia induzir um intérprete mais apressado a concluir que quaisquer meios aptos a demonstrar a evidência daqueles factos que se pretende colacionar no processo penal seriam admissíveis, desde que não recaíssem num óbice constante do artigo subsequente.

Na realidade, o ponto crucial da interpretação que deve ser dispensada ao dito artigo reside justamente na possibilidade de o encarar com uma aceção positiva[148]. Isso implica, do ponto de vista de uma hermenêutica sistemática, admitir que somente se poderia pretender arrecadar uma fonte de prova digital com recurso a meios invasivos ocultos, caso nenhum outro método fosse hábil a obter aquele resultado.

Nesse sentido, o investigador compreende que sejam acertados os termos selecionados por Maria Beatriz Seabra de Brito, quando defende como corolário do princípio da legalidade, que o «sistema de aquisição probatório» (art.º 125.º do CPP) seria «genericamente proibitivo» ou dependente de permissão legal expressa[149].

Deve aceitar-se, de um modo amplo, a premissa de que o art.º 4.º do CPP, apesar de admitir o uso da analogia, não autoriza a prática de aquisição de meios de obtenção de fontes de prova atípicos em sede de investigação de factos potencialmente enquadrados como delito penal «por constituir analogia empregada sempre *in mala partem*».[150]

O efeito de ineficácia de uma fonte de prova proibida resolve, igualmente, a questão doutrinária da teoria de finalidade de proteção da norma, que questiona se o sentido e o fim de uma disposição processual infringida requerem explicitamente uma proibição de utilização, resposta que entendemos ser evidentemente negativa[151].

Seguindo este ponto de vista, fica implícita uma reciprocidade entre proibição de produção e proibição de utilização, já que, quando o legislador proíbe a utilização de uma prova, está também a vetar, a montante, a sua produção.

Assim, verifica-se que o princípio da proporcionalidade deve guiar a atividade legislativa e judiciária, quando se pretenda prever que uma ferramenta como o *malware* possa ser empregada em sede de investigações criminais, e será ademais aplicável a todas as

[148]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 213
[149]BRITO, Beatriz Seabra de. *Novas Tecnologias e Legalidade da Prova No Processo Penal.* Coimbra: Almedina. 2018, p. 30
[150]Idem, p. 40
[151]AMBOS, Kai. «Las prohibiciones de utilización de pruebas en el processo penal alemán». AA.VV. *Prueba y Proceso Penal —Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado*. Valência: Tirant lo blanch. 2008, p. 343

esferas de atividade das entidades públicas, pautando cada ato com conteúdo decisório emanado da administração pública.

A jurisprudência da República Federativa do Brasil de 1988, por meio do Supremo Tribunal Federal, tem vindo a reafirmar que o postulado da proporcionalidade se qualifica como parâmetro de aferição da própria constitucionalidade material dos atos estatais[152].

Nesta hipótese, carece ao agente estatal encontrar por esta via benefícios condizentes com a extensão sacrificada de determinado direito, a revelar uma dimensão de adequação, como primeiro subprincípio e fomento ao objetivo que se pretende ver alcançado, na qualidade de resultado da ponderação.

Como um segundo subprincípio a ser levado em consideração durante a elaboração de normas pelo poder público, é possível conseguir alcançar a legitimidade do ato quando o âmbito da necessidade é respeitado. Esta vertente da necessidade, por seu turno, tem vindo a ser definida pelo Tribunal Constitucional Federal Alemão como o «objetivo não poder ser igualmente realizado por meio de outra medida, menos gravosa ao indivíduo»[153].

Segundo Gomes Canotilho[154], existem diversas particularidades que devem ser consideradas quanto ao critério de necessidade, para que o cidadão sofra a menor desvantagem. Estes aspetos são: a dimensão de exigibilidade material, pois o ato deverá implicar, na menor medida possível, a redução do âmbito de aplicação dos direitos fundamentais; a dimensão de exigibilidade espacial, que deverá demarcar com precisão o âmbito de aplicação das medidas restritivas; a dimensão de exigibilidade temporal, que remete ao lapso de tempo em que a restrição deverá ser aplicável; e, por fim, a dimensão pessoal, que exige a identificação das pessoas que eventualmente venham a ser atingidas pelo ato.

O último subprincípio que deve ser levado em consideração nesta ordem de avaliação fixa, inexorável e estabelecida previamente durante a elaboração ou aplicação de normas que venham a limitar direitos fundamentais é a proporcionalidade em sentido estrito (*stricto sensu*). Neste ponto, ressalvar-se-á a ponderação entre os meios que se pretende adotar e as finalidades que se pretende obter, e, ainda aqui, apesar de tal deter uma maior carga subjetiva

[152]BRASIL. Plenário do Supremo Tribunal Federal. ADI 5468/DF de 29/06/2016. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5468_voto_MCM.pdf (consultado pela última vez em 15/02/2021)
[153]ALEXY, Robert. *Teoria dos Direitos Fundamentais.* (V. A. Silva, Trad.) São Paulo: Malheiros Editores, LTDA. 2008, p.119
[154]CANOTILHO, José Joaquim Gomes. *Direito Constitucional e Teoria da Constituição.* Coimbra: Almedina. 2003, p. 270

por parte do decisor, os benefícios e os sacrifícios dos valores em causa deverão ser medidos e racionalmente aferíveis.

O princípio da subsidiariedade remete de volta ao subprincípio da necessidade e indica que, pelo potencial de lesão intrínseco ao método oculto, deverá sempre optar-se por um método aberto de investigação, caso seja suficiente para atender as finalidades de recolha das fontes de prova indispensáveis, e, mesmo dentre os métodos ocultos, deve optar-se por aquele que seja menos invasivo ou restritivo[155].

3.2. A restrição de direitos fundamentais durante o uso de *malware* como ferramenta de investigação estatal

Quando autoridades policiais ou judiciárias infiltram um programa espião num sistema informático, possibilitam o acesso expressivo à vida pessoal do visado e geram conflito com as seguintes posições *prima facie* estabelecidas: direito ao sigilo e proteção das comunicações (previstos no art.º 34.º, n.º 4, da CRP, no art.º 8.º da CEDH e no art.º 5.º, inciso XII, da CRFB/88); direito à reserva da intimidade (previsto no art.º 26.º, n.º 1, da CRP, no art.º 8.º da CEDH e no art.º 5.º, inciso X, da CRFB/88); direito à inviolabilidade do domicílio (previsto no art.º 34.º, n.º 1, da CRP, no art.º 8.º da CEDH e no art.º 5.º, inciso XI, da CRFB/88); direito à imagem e à palavra (previstos no art.º 26.º, n.º 1, da CRP e no art.º 5.º, inciso X, CRFB/88); direito à integridade e confidencialidade dos sistemas informáticos; direito à autodeterminação informativa.

A partir do instante em que se protege e se mantém o direito ao segredo das comunicações, sem que exista um receio de vigilância constante, assegura-se o «livre desenvolvimento da personalidade de cada um»[156], facultando o resguardo do processo de envio e recebimento de mensagens entre pessoas fisicamente distantes, no interesse da defesa da privacidade.

A relevância de se tratar aqui do direito ao segredo das comunicações reside, conforme visto acima, na possibilidade de ser encetada uma «vigilância na fonte»[157] com recurso a programas informáticos espiões que captam as condições e o teor da comunicação no

[155]ANDRADE, Manuel da Costa. «Métodos Ocultos de Investigação (Plädoyer para uma teoria geral)». AA.VV. *Que futuro para o Direito Processual Penal? Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*. Coimbra: Coimbra Editora. 2009, p. 546

[156]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, p. 158

[157]CAMPOS, Juliana. *O Malware como Meio de Obtenção da Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 15 (Versão eletrónica)

decurso da sua marcha dinâmica, tornando absolutamente ineficazes medidas de autoproteção, como a criptografia[158].

O direito ao segredo das comunicações traduz a impossibilidade de intrusão de terceiros não participantes ou não autorizados por estes a participarem do ato comunicacional, incluindo o Estado, para conhecimento das condições em que se desenvolveram comunicações efetuadas entre quaisquer interlocutores (dados de tráfego), bem como acerca do seu conteúdo. O processo comunicativo estará consumado quando os dados forem efetivamente recebidos pelo destinatário, independentemente da sua leitura, passando a valer como mais um ficheiro armazenado no sistema informático ou um normal escrito, não implicando a sua apreensão na mitigação do direito sob análise[159]. Quaisquer interceções não autorizadas pelo poder judiciário serão ilícitas, em especial quando estiverem a ser utilizados instrumentos tecnológicos de vigilância com a finalidade de antever e combater crimes.

No que respeita ao direito à reserva da intimidade, emanando diretamente da dignidade da pessoa humana[160], observa-se um espetro de irradiação amplo, já que é um direito que abarca todos os aspetos relacionados com manifestações da esfera íntima, privada e da personalidade[161].

O autor Daniel J. Solove[162] liga a intimidade à possibilidade de o sujeito se opor a intromissões não autorizadas na esfera privada.

Naturalmente, a vida privada está abrangida na esfera íntima da pessoa, porém não servirá para delimitar toda a extensão do que pode ser considerado a intimidade de um indivíduo. Na sua faceta de direito à autopreservação, alcança inclusive o direito de ser «deixado em paz», de permitir que se mantenha isolado, distante de olhares curiosos de outros, tomando as suas decisões pessoais sozinho («Right to be alone»).

Para reavivar as noções de limites passíveis de intrusão, a jurisprudência alemã elaborou a teoria dos três graus, com especial foco no direito à intimidade. Clarificou que existiriam três esferas concêntricas, em que a primeira, mais interior, consistiria no núcleo

[158]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, p. 165

[159]«A proteção a que se refere o art.º 5.º, XII, da Constituição é a da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador». (Brasil, Supremo Tribunal Federal. RE 418.416/SC, rel. Min, Sepúlveda Pertence, DJ 19.10.2006)

[160]NOVELINO, Marcelo. *Manual de Direito Constitucional* — 8.ª ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: MÉTODO. 2013, p. 489

[161]SILVA, José Afonso da. *Curso de Direito Constitucional Positivo* — 32.ª ed. rev. e atual. São Paulo: Malheiros. 2009, p. 206

[162]SOLOVE, Daniel J. *Conceptualizing Privacy*. Califórnia: California Law Review. 2002, p. 1092

essencial inviolável e absolutamente inalcançável, mesmo pelas instâncias formais de controlo, retirado também da ponderação legislativa. Estariam aí abrangidos sentimentos íntimos, a identidade sexual, diários pessoais e conversas familiares e de confissão religiosa[163]. A segunda esfera estaria já sujeita a interferências devido a necessidades da comunidade política, como, por exemplo, quebras de sigilos bancários e fiscais[164]; e a terceira e maior das esferas corresponderia a um campo em que as interferências já seriam aceites, por constituírem o âmbito da vida social, aquilo que já seria naturalmente público no seu contexto social[165].

O *malware* é capaz de atentar contra o núcleo inalcançável da esfera da intimidade, uma vez que pode arrecadar informações armazenadas que reflitam uma fotografia completa da personalidade individual, uma representação fidedigna da vida psicológica e física do investigado, tendo como exemplo um diário íntimo mantido em formato digital.

Caso se utilizasse *software* malicioso para ativar remotamente *hardware* de um sistema informático e respetivas funções, como as da câmara ou do microfone, sem dúvida que se desnudariam e tornariam públicas inúmeras particularidades da vida privada alheia, uma medida potencialmente lesiva e restritiva do núcleo inalcançável da intimidade, que não se justificaria pela busca de eficiência do processo penal[166].

As Constituições dos Estados liberais previram também a proteção contra violações ilegais ao domicílio. Identificado tradicionalmente pelos limites do imóvel que constitui a residência, ou pelo espaço físico limitado pela soleira da porta de entrada, este é um direito fundamental de primeira dimensão.

Sendo «o domicílio o espaço normal da intimidade»[167], é o local onde, naturalmente, os comportamentos se desenvolvem de maneira franca e irreprimível. Não obstante, o domicílio não está necessária e exclusivamente associado ao conceito de habitação, podendo inclusive ser temporário. Pode, por exemplo, ser um quarto de hotel, um leito individual de hospital, ou, num contexto profissional, um escritório.

---

[163]CAIRES, João Gouveia de. «O registo de som e imagem e as escutas ambientais». AA.VV. *Direito da Investigação Criminal e da Prova*. Coimbra: Almedina. 2014, p. 494

[164]NOVELINO, Marcelo. *Manual de Direito Constitucional* — 8.ª ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: MÉTODO. 2013, p. 490

[165]CORREIA, João Conde. «Questões práticas relativas à utilização de diários íntimos como meio de prova em processo penal». *Revista do CEJ*, n.º 5. 2007, p. 148 — 150

[166]MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Salvador: Editora JusPodivm. 2020, p. 95

[167]ANDRADE, Manuel da Costa. «Domicílio, intimidade e constituição: anotação crítica ao Acórdão 364/2006 do Tribunal Constitucional». *Revista Brasileira de Ciências Criminais*, Vol. 100. São Paulo. Jan. – fev. de 2013, p. 71

No caso de necessidade de entrada pessoal do agente de investigação no domicílio, para efeitos de instalação de *malware* com precisão no sistema informático do visado, o primeiro conflito apresentar-se-ia de modo patente. Este dano ao direito fundamental pode, eventualmente, vir em conjunto com outras tecnologias utilizadas para incrementar um afã punitivo.

Tampouco se pode avaliar que a intromissão, e consequente lesão do valor jurídico, somente ocorre de modo pessoal e corpóreo, sendo perfeitamente viável e possível uma intrusão e vigilância de modo eletrónico-digital[168]. São exemplos fáticos da quebra de uma barreira acústica a utilização de microfones de longo alcance desde o exterior do domicílio, e da demolição de uma barreira visual o recurso a filmagens do interior do imóvel por meio de um veículo aéreo não tripulado, usado como base para a proceder às mesmas.

É importante não olvidar que informações mais relevantes e íntimas estão hoje armazenadas em sistemas informáticos, e que uma eventual divulgação das mesmas seria, possivelmente, mais reveladora da intimidade de um indivíduo do que uma revista específica à casa onde se desenvolve a sua vida conjugal. Existem inclusivamente menções doutrinárias a um domicílio virtual composto por tais informações[169].

A vigilância não atinge a inviolabilidade domiciliar caso o *malware* seja instalado remotamente e à distância, sendo utilizado para recolher apenas dados internos do sistema, ainda que voláteis e presentes apenas na memória temporária do dispositivo.

Apesar de se revelar possível fustigar o direito à inviolabilidade do domicílio por meio do uso de *software* malicioso, quando acionadas de modo remoto e telemático partes do *hardware* como câmaras e microfones, deve-se considerar que grande parte dos dispositivos de processamento de dados eletrónico-digitais utilizados hodiernamente são móveis, enquanto este direito foi concebido para proteger uma realidade física estanque. Tal facto poderia levar a paradoxos, pois o utilizador ficaria concomitantemente protegido e desprotegido durante a execução de determinada atividade, bastando para tanto abandonar os limites do imóvel.

Para admitir qualquer agressão advinda de uma investigação criminal ao direito perquirido, será necessária ao magistrado a observância do princípio da especialidade, fundamentada na existência de evidências que especifiquem a ocorrência de um delito, não

[168]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, p. 151

[169]MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Salvador: Editora JusPodivm. 2020, p. 224

sendo viável a sua imolação para investigações prospetivas ou para a concretização de uma *fishing expedition.* Será obrigatoriamente considerado o princípio da adequação, que deverá ser demonstrado a partir da verificação do prazo de duração da medida e da utilidade fática do seu resultado.

Igualmente necessário será o acatamento do princípio da excecionalidade, indicando a inexistência de outra medida menos invasiva que se preste ao mesmo fim de elucidar a verdade dos factos, demonstrando a imprescindibilidade correlata ao grau de lesão potencial de um método oculto, como a intrusão por código arbitrário[170].

Os direitos à palavra e à imagem são autónomos[171] e decorrem diretamente do direito à reserva da intimidade e da necessidade de preservação da identidade pessoal legalmente resguardada. Tais direitos pretendem impedir a captação e difusão da palavra e da imagem, respetivamente, sem o consentimento do titular, já que a palavra falada cria uma expectativa de que seja transitória, pela sua natureza intrínseca, normalmente ouvida apenas durante a oportunidade em que se faz uso da fala. Além disso, as palavras faladas que não sejam publicamente armazenadas permanecem na esfera da disponibilidade do titular e possibilitam-lhe a eleição do público ouvinte, pelo que lhe competirá de modo soberano a seleção do auditório a vincular o território onde as professou.

As palavras faladas são objeto de proteção inclusive em locais públicos em que se travem conversas privadas, sendo igualmente inviável a sua obtenção como fonte de prova, caso se constitua em sons sem conversação, solilóquio, e comunicação verbal resguardada por norma de sigilo profissional, impedindo a sua montagem ou descontextualização, com o intuito de evitar que o processo penal se degenere em mera formalidade, e o indivíduo em seu objeto.

Sem o consentimento do titular ou prévia autorização judicial, está vedada a captura e exposição da imagem exterior de um arguido, na mesma medida em que o Estado estaria impedido de utilizar imagens ofensivas à autorrepresentação constante de fotografias ou vídeos armazenados na memória interna de sistemas físicos ou virtuais, obtidos através de penetração por *software* malicioso.

O mesmo se diga da ativação remota das funcionalidades de *hardware* do sistema informático, como câmaras e microfones, relevando em especial o local e tempo de duração

[170]MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Salvador: Editora JusPodivm. 2020, p. 224

[171]CAIRES, João Gouveia de. «O regime processual especial aplicável ao crime organizado (económico-financeiro): âmbito de aplicação da Lei n.º 5/2002, de 11 de Janeiro, o regime do sigilo e do registo de voz e imagem». AA.VV. *Direito Penal Económico e Financeiro.* Coimbra: Coimbra Editora. 2012, p. 523

da medida, posto que, caso ocorra no interior do domicílio, representará uma violação que tenderá a afetar todo o material probatório recolhido[172].

Já que os surgimentos de novos direitos fundamentais não funcionam sob condição da reserva de um progresso técnico-científico, a autodeterminação informativa (*Grundrecht auf informationelle selbstbestimmung*) foi reconhecida por uma dedução constante da decisão do Tribunal Constitucional Federal Alemão, no contexto de um processo acerca do censo demográfico que decorreu naquela nação em 1983, denominado *Volkszahlungsurteil*[173].

Refere-se ao poder conferido às pessoas para saberem quem teria acesso aos seus dados pessoais, de que forma, com que objetivo e sob que circunstâncias se facultaria este conhecimento para análise. O direito à autodeterminação informativa apresenta-se como medida de proteção de tais dados, formulando-se como o direito pessoal que cada sujeito detém na determinação do destino dos seus dados e suas retransmissões[174]. No âmbito do direito geral da personalidade, são estabelecidas regras para o processamento estatal e privado dos dados pessoais que visam englobar uma proteção de natureza dinâmica e impedir que o indivíduo seja manipulado por informações que os seus interlocutores possuam a seu respeito, sem o conhecimento do titular de interesses.

O Tribunal Constitucional Alemão compreendeu que a proteção de dados seria um pré-requisito para que um cidadão aderisse a atividades públicas, como reuniões políticas ou sindicais, possibilitando que os indivíduos exercessem o seu papel social ativamente, na medida em que estabelece os limites para uma comunicação democrática.

A proteção dos dados está relacionada com os princípios norteadores da correção, da exatidão, da publicidade, do acesso individual e da segurança, interpretados de forma a impedir um excessivo controlo estatal[175].

O direito em voga não estabeleceu que os dados seriam uma propriedade do titular de interesses, mas um ordenamento que disciplina as informações contidas em contextos comunicacionais e o seu respetivo tratamento. O Estado não poderia adentrar e trespassar

[172]MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Salvador: Editora JusPodivm. 2020, p. 201

[173]MENKE, Fabiano. «A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão». AA.VV. MENDES, Gilmar F.; SARLET, Ingo W.; COELHO, Alexandre Z. P. *Direito, Inovação e Tecnologia.* São Paulo: Saraiva. 2015 (Versão eletrónica)

[174]ROMERO SANCHEZ, Angelica. «Proceso penal, privacidad y autodeterminación informativa en la persecución penal de la delincuencia organizada. Un análisis desde la perspectiva del derecho procesal penal alemán.» *Revista Criminalidad*, Vol. 57(2): 319 — 335. 2015, p. 326

[175]MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Salvador: Editora JusPodivm. 2020, p. 220 – 221

furtivamente, de modo escondido e fraudulento, num sistema informático, para recolher dados, por exemplo, relativos a uma consulta médica.

Na abordagem de Nicolás González-Cuéllar Serrano[176], haveria um verdadeiro direito à não intromissão no domínio digital, reconhecido pelo Supremo Tribunal Espanhol, pelo menos desde a resolução 342/2013.

De facto, o uso de *software* estatal voltado para espionagem pode agredir o direito sob análise, posto que, ocasionalmente, permitirá ao recetor dos dados traçar um perfil completo do investigado. Não obstante, este mesmo direito é incapaz de efetivar uma proteção suficiente que lhe permita lidar com a complexidade dos sistemas de tecnologia da informação e comunicação.

Conforme explorado no capítulo 2.3, o Tribunal Constitucional Federal Alemão estabeleceu um novo direito fundamental à integridade e confidencialidade dos sistemas informáticos (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*), em decisão datada de 27 de fevereiro de 2008, com a intenção de proteger os indivíduos contra as mais modernas ameaças à personalidade.

Após verificar a possibilidade concreta de uma investigação estatal se socorrer de *software* malicioso, com acesso integral a todos os aspetos do sistema, a corte constitucional escreveu um importante capítulo na história da proteção de dados e consagrou um novo direito com o objetivo de resguardar, de modo amplo, dispositivos que possuam como requisitos mínimos os recursos de processamento e armazenamento de dados ou que possam estar ligados a uma rede[177]. Para o efeito, observou que os utilizadores não estariam protegidos por outros direitos fundamentais convencionais tradicionalmente positivados, como a privacidade de correspondência, correios, e outros já acima mencionados.

O prisma da confidencialidade está voltado para proteção dos dados criados, processados ou armazenados pelos utilizadores de sistemas de modo voluntário ou automático[178], a exemplo do objetivo do direito à autodeterminação informativa, com o diferencial que os requisitos para sua mitigação sejam mais exigentes. O viés da integridade

[176]GONZÁLES-CUÉLLAR SERRANO, Nicolás. «Garantias constitucionales de la persecución penal en el entorno digital». AA.VV. COLOMER, Juan Luis Gómez. *Prueba y Proceso Penal (Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado*. Valência: Tirant to Blanch. 2008, p. 181 – 182

[177]HORNUNG, Gerrit; SCHNABEL, Christoph. «Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention». *Computer Law & Security review*, Vol. 25, n.º 2. 2009, p. 116

[178]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». *In Madhuri, Vol. 9; Hacking. ICFAI University Press*. Vol.6 (1): 167 – 191. Abril de 2009, p. 120

foi estabelecido com a intenção de «proteger contra o uso não autorizado do sistema no que diz respeito às suas capacidades, funções e conteúdos de memória».[179]

Isso significa que foi pretensão efetiva do Tribunal proteger o titular de interesse contra o acesso clandestino a um sistema informático passível de invasão, ou quaisquer outros sistemas que sejam acessíveis a partir do inicial, como *webmails* e outros serviços de computação em nuvem[180], na sua totalidade ou a qualquer de suas partes sensíveis, inclusivamente informações inseridas que não precisariam de vir a ser processadas, mas que poderiam ser adquiridas por meio de *key-loggers*[181].

[179]HORNUNG, Gerrit; SCHNABEL, Christoph. «Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention». *Computer Law & Security review*, Vol. 25, n.º 2. 2009, p. 116

[180]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 248

[181]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». *In Madhuri, Vol. 9; Hacking. ICFAI University Press.* Vol.6 (1): 167 – 191. Abril de 2009, p. 121

4. TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO, PRESSUPOSTOS PARA RECOLHA DA PROVA DIGITAL E AS MEDIDAS ANTIFORENSES

4.1. Tecnologias da informação e comunicação (TIC)

As novas tecnologias disponibilizam recursos que acrescentam capacidade aos sentidos, na medida em que transformam a presença física, os gestos, e ampliam a capacidade de memória em *bits*, armazenando informações massivamente, numa penetração profunda no quotidiano dos cidadãos.

As tecnologias da informação baseiam-se maioritariamente na *Internet* e nos respetivos protocolos de comunicação de rede[182]. É possível enviar mensagens de modo instantâneo a um vasto conjunto de pessoas.

É oportuno esclarecer, nesta altura, ainda que de modo superficial e sem pretensão de exaustividade, o funcionamento do ciberespaço. Já que a parte mais relevante em investigações criminais que façam uso de *malware* tende a ocorrer *on-line*, fará todo o sentido que se explore o meio no qual estas se desenvolvem.

Longe de ser um espaço físico, o ciberespaço é um meio de comunicação. De uma perspetiva material, a *Internet* requer condições de existência dos equipamentos indispensáveis para que o tráfego de dados ocorra, como: cabos, fios, satélites e outros, com a finalidade de ligar entre si os seus utilizadores[183].

Arquitetada para funcionar como uma tecnologia que propiciasse uma comunicação constante e livre[184], a *Internet* precisou de protocolos de comunicação padronizada, sendo atualmente utilizado o TCP/IP (*Transmission Control Protocol/Internet Protocol)*. Os dados são transferidos entre as redes pela sua conversão entre os diferentes sistemas, servindo o endereço IP para mostrar onde estes dados devem ser entregues[185].Tal endereço é atribuído automaticamente pelos provedores de serviços de *Internet* (ISP) cada vez que um utilizador a ela se conecta[186,187].

---

[182]Constituindo-se em regras para comunicação entre os nós de uma rede (MARTÍNEZ MARTÍNEZ, Ricard. «En torno a la consideración jurídica del numero IP». *Anuario Multidisciplinar para la modernización de las Administraciones Públicas*, n.º 1. 2005, p. 284)

[183]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 51

[184]CASTELLS, Manuel. *A Galáxia Internet — Reflexões sobre internet, negócios e sociedade*. Rio de Janeiro: Zahar. 2003, p. 10 — 11

[185]MARTÍNEZ MARTÍNEZ, Ricard. «En torno da la consideración jurídica del numero IP». *Anuario Multidisciplinar para la modernización de las Administraciones Públicas*, n.º 1. 2005, p. 284.

[186]Concelho da Europa. *Electronic Eviden–e Guide — A basic guide for police officers, prosecutors and judges — Versão 1.0.* 2013, p. 186

[187]Idem, p. 96

A adoção do número IP permite a localização dos sistemas informáticos ligados em rede[188], e dá detalhes do dispositivo e do contrato de serviço que vincula o internauta ao provedor de serviços de *Internet*[189,190], podendo ser atribuído um número estático ou dinâmico e ainda a fragmentação dos dados em pacotes para entrega ao destinatário final, sem que exista um trajeto rígido.

O TCP complementa estas funções, o controlo do protocolo de transmissão está sempre voltado para a comunicação, possuindo a função de garantir a entrega e reestruturação dos pacotes de dados na ordem correta, desde a requisição do cliente até a entrega pelo servidor, solicitando ao remetente novo envio caso «qualquer pacote se perca no percurso»[191].

Um enorme número de dispositivos eletrónico-digitais foi desenvolvido para facultar o acesso direto e ininterrupto a esta rede de redes que é a *Internet*[192], tais como *smarthphones*, computadores portáteis, câmaras, consolas de videojogos e diversos outros aparelhos com semelhantes funções.

Ressalta-se aqui que o conceito de dispositivo eletrónico é mais amplo do que o conceito de dispositivo digital[193], abrangendo aqueles que produzem dados analógicos, como uma câmara que produz uma filmagem numa fita de vídeo[194].

Os dados digitais que compõem as comunicações em rede por meio de *bits* estão atualmente armazenados nos dispositivos físicos citados ou em meios virtuais (*on-line*), através de sistemas de computação em nuvem (*cloud computing*), «podendo ser provisionados e liberados sob demanda»[195].

4.2. Pressupostos para a recolha da prova digital: a cadeia de custódia

[188]ORTIZ PRADILLO, Juan Carlos. «Fraude y anonimato en la red: cuestiones constitucionales y procesales de la desanonimización de la red TOR». AA.VV. C. S. Crespo, Fraude Electrónico – *Su gestión penal y civil.* Valência: Tirant to Blanch. 2015, p. 46 — 47 (Versão eletrónica)
[189]Concelho da Europa. *Electronic Eviden–e Guide — A basic guide for police officers, prosecutors and judges — Versão 1.0.* 2013, p. 97
[190]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 54
[191]Idem, p. 55
[192]MARTÍNEZ MARTÍNEZ, Ricard. «En torno da la consideración jurídica del numero IP». *Anuario Multidisciplinar para la modernización de las Administraciones Públicas*, n.º 1. 2005, p. 284
[193]SALT, Marcos. *Nuevos desafios de la evidencia digital: acceso transfronteirizo y técnicas de acceso remoto a datos informáticos* — 1.ª ed. Buenos Aires: Ad-hoc. 2017, p. 31 (Versão eletrónica)
[194]RODRIGUES, Anabela Miranda. *Inteligência Artificial no Direito Penal*. Edições Almedina. 2020, p. 59 (Versão eletrónica, acessível em: https://ebooks.almedina.net/books/9789724089676)
[195]BADGER, Lee; GLANCE, Tim; PATT-COMER, Robert; VOAS, Jeff. «Cloud computing synopsis and recommendations». *NIST Special Publication*. Maio de 2012, p. 2 — 1 (Tradução livre)

O processo criminal é o percurso necessário para a imposição de uma pena, ficando o controlo dos seus passos sob as rédeas do Poder Judiciário, no escopo da concretização do projeto democrático. Com vista a atingir este objetivo, e dada a evolução das TIC, introduziu-se numa grande quantidade de procedimentos criminais, a valoração técnica de vestígios constituídos por «impulsos digitais»[196] elétricos.

O método do *software* malicioso oculto colocado no centro de uma investigação policial provoca uma mudança de paradigma quanto à forma de obter fontes de meios de prova diretamente no equipamento informático ligado ao arguido, de modo bastante rápido e eficaz, em especial atendendo às rotineiras buscas e apreensões de suportes físicos.

Sendo os *bits* passíveis de serem tratados como provas valoradas processualmente, dá-se, então, origem a um novo conjunto de regras e princípios de observância obrigatória, designado por Ciência Forense Digital (*Digital Forensics Science*), acerca da qual é relevante expor alguns pontos. Conforme ressalta Carlos Hélder C. F. Mendes, esta ciência forense «agrega mecanismos na investigação de crimes relacionados com computadores, adequadamente às disposições constitucionais e às leis de Direito Processual Penal»[197].

O Estado deverá levar a efeito um conjunto de passos metódicos, como condição indispensável para efetivar quaisquer tratamentos de dados eletrónico-digitais apreendidos durante atividade na seara criminal. Este tratamento consiste em qualquer ação com a finalidade de proceder a

> «pesquisas, recolhas, registos, organização, classificação, comparação, valoração, conservação, modificação, adaptação, alteração, recuperação, consulta, utilização, transferência, transmissão, interconexão, bloqueio, descarte ou destruição de quaisquer informações»[198],

inclusivamente quando, diante de dados obtidos em sede de investigação criminal oculta, que tenha lançado mão de códigos arbitrários.

Neste sentido, a Associação dos Chefes de Polícia da Inglaterra, País de Gales e Irlanda do Norte (*Association of Chief Police Officers* — ACPO) estabelece como princípios aplicáveis durante a manipulação de prova digital os seguintes:

> «nenhuma ação tomada por agências de aplicação da lei, pessoas ou agentes empregados nessas agências deve alterar dados que possam ser posteriormente invocados em

[196]LÁZARO DOMÍNGUEZ, Francisco. *Introducción a la Informática Forense.* Madrid: Ra-Ma. 2013, p. 21
[197]MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Salvador: Editora JusPodivm. 2020, p. 113
[198]Projeto de Lei do Senado n.º 33, de 2013, Artigo 3.º, §2.º, da República Federativa do Brasil (Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/113947; consultado pela última vez em 05/07/2020)

> tribunal; que nas circunstâncias em que uma pessoa considere necessário aceder a dados originais, essa pessoa deve ser competente para fazê-lo e ser capaz de fornecer evidências explicando a relevância e as implicações das suas ações; que uma trilha de auditoria ou outro registo dos processos aplicados à evidência digital deve ser criada e preservada de modo a facultar que um terceiro independente seja capaz de examinar estes processos alcançando o mesmo resultado; e que a pessoa encarregada da investigação possui a responsabilidade geral de garantir o cumprimento da lei e destes princípios»[199].

A Ciência Forense Digital é uma das vertentes da ciência forense, estando conceituada pelo *National Institute of Standards and Technology* (NIST), do Departamento de Comércio do governo norte-americano, como sendo a técnica voltada para a «aplicação da ciência à identificação, coleta, exame e análise de dados, preservando a integridade das informações e mantendo uma cadeia estrita de custódia para os dados»[200].

Conforme aponta David Silva Ramalho, a Ciência Forense Digital engloba diversas categorias, como «as Ciências Forenses de Redes (*network forensics*), de Dispositivos Móveis (*mobile devices forensics*), de Intrusão (*intrusion forensics*) ou de *Malware* (*malware forensics*), entre outras».[201]

Existem variações terminológicas no conceito de Ciência Forense Digital por parte da literatura especializada, sendo possível absorver como cerne desta diversidade de classificações as ações de «identificar, preservar, analisar e apresentar evidência digital de uma maneira que seja aceitável em processos judiciais»[202].

O momento inicial será indubitavelmente o processo de identificação, que consiste em reconhecer os indícios de autoria ou, pelo menos, o sistema informático utilizado para execução do delito, em que se constrói uma narrativa da dinâmica dos eventos *contra legem*. A partir daí, com a autorização judicial em mãos, o investigador digital estará apto a dar passos para tratar uma prova digital que possua os atributos da integridade e confiabilidade.

---

[199]Association of Chief Police Officers. *ACPO Good Practice Guide For Digital Evidence* — 4.ª ed. 2012, p. 6 (Disponível em https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf; consultado pela última vez em 06/05/2020) (Tradução livre)

[200]KENT, Karen; CHEVALIER, Suzane; GRANCE, Tim; DANG, Hung. «Guide to Integrating Forensic Techniques into Incident Response». *NIST Special Publication 800-86*, Maryland: NIST. 2006; p. 2 — 1 (Tradução livre)

[201]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 111

[202]GUO, Yinghua; SLAY, Jill. «Data recovery function testing for digital forensic tools». Kam-Pui CHOW; Sujeet SHENOI, *Advances in Information and Communication Technology.* Berlim: Springer. 2010, p. 297 (Tradução livre)

Esta ciência surge traduzindo a necessidade de observar valores básicos de organização, para evitar a inutilização da fonte de meio de prova, que, pela respetiva fragilidade e volatilidade, é suscetível de ser alterada[203]. Em qualquer circunstância, o investigador digital necessita do uso de engenho, devendo, contudo, cumprir uma metodologia em cada etapa da cadeia de custódia que permita a usabilidade da prova.

A referência a «investigador digital» em detrimento do termo «perito» advém precisamente de o momento de investigação corresponder, regra geral, ao curso de um inquérito prévio ao processo penal. Apesar de ambos os profissionais serem dotados das mesmas competências e habilidades técnicas, não se trata, neste caso, de uma perícia tradicional.

A perícia poderá ser ordenada pelo magistrado judicial e seguirá procedimentos próprios da fase processual que se desenvolve em contraditório, a exemplo da nomeação de assistentes técnicos. Salienta-se que esta perícia, que advirá noutra etapa processual, deve fazer uso do material recolhido remotamente, já previamente analisado pela investigação criminal, e trabalhar sobre ele.

Posteriormente, ganhará importância para a adequação técnica com os requisitos da prática forense digital, um verdadeiro desenho do modo através do qual se deve montar o conjunto que formará a silhueta de um procedimento de coleta. De acordo com o modelo proposto pelo NIST, este será seguido dos procedimentos de exame, análise e relatório.

Assim, torna-se indispensável realizar cópias do sistema informático por inteiro. O autor defende que todo o sistema informático seja copiado de modo integral apenas por razões de segurança de todos os envolvidos, tendo em vista o princípio do contraditório e ampla defesa que se estabelecerá no seguimento, sem que tal signifique que a ordem judicial faculte o acesso a todas as informações ali existentes. O modelo acima citado, não obstante, leva a ressaltar que existem casos em que a quantidade massiva de dados tornará esta medida impraticável[204].

Tendo em consideração a capacidade de o *malware* obter toda a informação que passa pelo processador de dados do sistema informático, o que permite ao intruso estatal o

[203]RODRIGUES, Benjamim Silva. *Da Prova Penal – Tomo IV – Da Prova Electrónico-Digital e da Criminalidade Informático-Digital.* Lisboa: Rei dos Livros. 2011, p. 42

[204]KENT, Karen; CHEVALIER, Suzane; GRANCE, Tim; DANG, Hung. «Guide to Integrating Forensic Techniques into Incident Response». *NIST Special Publication 800-86*, Maryland: NIST. 2006, p. 3 — 4 (Tradução livre)

conhecimento do que o «utilizador escreve, lê, vê e faz»[205], as cópias integrais aparentam ser o modo mais seguro de garantir inclusivamente o sucesso de uma tese defensiva.

Cópias de quaisquer materiais probatórios digitais destinados a processos judiciais e decorrentes de buscas e apreensões devem ser necessariamente assegurados com a geração da chamada função *hash (message digest)*[206]. Esta é uma técnica de criptografia, ao lado da cifragem de chave simétrica e assimétrica, à qual se fará referência no tópico seguinte[207].

O autor Michael Sheetz aduz que «basicamente, o *hashing* pode ser conceituado como o equivalente a uma impressão digital»[208] e acrescenta que, do ponto de vista científico, o *hashing* estabelece uma certeza de que dois objetos digitais não devem jamais possuir valores idênticos. Afirma ainda que se um único *bit* for alterado, o programa calculará um valor *hash* totalmente diferente para o ficheiro, na mesma medida em que duas pessoas não têm impressões digitais idênticas.

De modo mais aprofundado, Donald Justin Price dá conta de que o código *hash* é um algoritmo matemático que pode ser usado para «autenticar ou comparar imagens digitais». A função *hash*, também conhecida como MD-5, consiste numa forma algébrica racional inteira em formato binário que gera uma «sequência numérica única»[209].

Durante a etapa de aquisição das informações constantes do entorno virtual do visado, os dados serão considerados voláteis sempre que se perderem com a passagem do tempo ou que possam vir a ser perdidos, a partir de outras ações executadas no sistema informático, a exemplo do comando de desligamento, reinício do equipamento ou ainda como consequência do processo decorrente do fim da fonte de energia elétrica. Neste ínterim, tal modalidade de dados deve ser considerada prioridade pelo investigador digital no momento da recolha[210].

Assim, a decisão judicial servirá como uma referência a partir da qual se oferecerá ao analista um plano por escrito, contendo linhas de ação e procedimentos, para que este profissional especialista em informática exerça as suas prioridades de modo eficiente,

[205]KERR, Orin S. «Searches and seizure in a digital word». *Harvard Law Review*, Vol. 119. 2005, p. 532
[206]SHEETZ, Michael. *Computer Forensics: An Essential Guide to Accountants, Lawyers and Managers.* Nova Jérsia: John Wiley & Sons. 2007, p. 113
[207]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017, p. 168
[208]SHEETZ, Michael. *Computer Forensics: An Essential Guide to Accountants, Lawyers and Managers.* Nova Jérsia: John Wiley & Sons. 2007, p. 113 (Tradução livre)
[209]PRICE, Donald Justin. «The analog and digital word». AA.VV. J. J. Barbara, *Handbook of Digital and Multimedia Forensic Evidence*. Nova Jérsia: Humana Press. 2008, p. 7 (Tradução livre)
[210]KENT, Karen; CHEVALIER, Suzane; GRANCE, Tim; DANG, Hung. «Guide to Integrating Forensic Techniques into Incident Response». *NIST Special Publication 800-86*, Maryland: NIST. 2006, p. 3 — 2 e 3 — 3 (Tradução livre)

evitando o manuseio incorreto ou a adulteração das informações[211]. Deste ponto, é preciso realçar que a informação recolhida deverá manter-se arquivada, com vínculo a fichas pessoais de todos os trabalhadores que detiveram a custódia do material recolhido, sendo que aquele mesmo manifesto deve prever expressamente a autorização para aquisição remota de dados, ao verificar a possibilidade ou necessidade de obtenção de informações por inúmeros sistemas e por meio de diversas conexões.

Todas as ferramentas de *software* utilizadas devem possuir um registo detalhado, incluindo as técnicas de *malware* operadas para conseguir o acesso ao interior do sistema informático, contendo o seu código fonte, tudo em benefício da repetibilidade.

Mantido o registo da intrusão em si mesma, o trabalhador governamental que o efetivou deve apresentá-lo, assim como tal registo deverá conter a data e o horário do seu princípio e fim. Caso esta intrusão seja efetuada numa rede empresarial de uma organização de médio ou grande porte, os administradores não suspeitos deverão ser contactados e as informações fornecidas documentadas[212].

Seguindo para a fase de exame, o especialista informático deve selecionar os arquivos que possuem interesse para a investigação. Neste procedimento, procura-se peneirar e filtrar os dados e o investigador poderá usar ferramentas que auxiliem a identificação do tipo de ficheiro, como textos, áudios, imagens etc.[213]

Concluída a seleção dos ficheiros relevantes para a investigação criminal, os dados passarão por um estudo que permita a retirada de conclusões que importem para o inquérito policial, como a identificação de pessoas, locais e eventos, documentando cada detalhe encontrado e especificando as ações tomadas para a descoberta. Esta etapa de análise leva a que, a partir dos elementos digitais, o investigador possa compreender o que se passou no mundo material.

Todos os eventos anteriores estarão consubstanciados no último momento, que consistirá na elaboração de um relatório com o objetivo de apresentar uma hipótese para a dinâmica do crime e, caso sejam viáveis, explicações alternativas. Eventualmente, caso os dados demonstrem o planeamento de execução de determinada infração futura, o relatório poderá indicar ações para a interrupção da mesma.

Aquilo que foge aos olhos do utilizador sem competências em tecnologias da informação e comunicação é trazido por Stephen Mason, quando afirma que metadados

[211]Idem, p. 3 — 3
[212]Idem, p. 3 — 3
[213]Idem, p. 3 — 6

(*metadata)* são «essencialmente, dados sobre dados». O autor afirma que todos os documentos eletrónico-digitais possuem metadados, desde um *e-mail* enviado, até *websites* e folhas de cálculo, e servem para auxiliar na identificação do destino da sua natureza. Avaliando os metadados de modo mais amplo, são, de um modo geral, elaborados de modo instantâneo pelo *software*, muitas vezes sem interferência do utilizador. Mason deixa expresso que, em especial no caso de o usuário não ser proficiente em ciência informática, este não saberá onde se situam tais informações e, mesmo que descubra a localização das mesmas, não as poderá «alterar, manipular ou excluir»[214].

Aquilo que pode ser obtido a partir de uma pesquisa cuidada por estas informações de base pode ser exemplificado

> «por quando e como um documento foi criado (hora e data indicadas), o tipo de arquivo, o nome do suposto autor (embora isso não seja necessariamente confiável), o local onde o ficheiro foi aberto ou onde foi armazenado, quando o mesmo foi pela última vez aberto (hora e data sugeridas), quando foi modificado pela última vez, quando o ficheiro foi guardado pela última vez, quando foi impresso pela última vez, a identidade dos supostos autores anteriores, a localização do ficheiro em cada ocasião em que foi armazenado, os detalhes de quem mais pode obter acesso a ele e, no caso de *e-mail*, endereços de cópia oculta»[215].

Não obstante, o mencionado escritor ressalta que os metadados são dotados de um nível de falibilidade para o investigador digital, para em seguida observar, no seu trabalho, que o técnico deve avaliar as circunstâncias em que os mesmos foram gerados, pois, se o relógio ou o fuso horário tiverem sido alterados, os dados gerados e registados serão falsos. Além disso, o autor assinala que os metadados podem ser removidos, desde que se faça uso de *software* especializado[216].

Pode, igualmente, confirmar-se a imprescindibilidade de recorrer a um especialista em Ciência Forense Digital, pela observação da eventual necessidade de recuperação de ficheiros que tenham sido «total ou parcialmente danificados, corrompidos, apresentem falha ou sejam por alguma razão inacessíveis na sua memória e dispositivos avulsos de armazenamento»[217].

---

[214]MASON, Stephen; SENG, Daniel Seng (eds.). *Electronic Evidence* — 4.ª ed. London: Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London. 2017, p. 27 – 32. (Tradução livre)

[215]Idem

[216]Idem

[217]GUO, Yinghua; SLAY, Jill. «Data recovery function testing for digital forensic tools». Kam-Pui CHOW; Sujeet SHENOI, *Advances in Information and Communication Technology.* Berlim: Springer. 2010, p. 299

Equívocos basilares podem trazer grandes prejuízos para a fase judicial, como na circunstância de o especialista transcrever incorretamente um número IP ou gravar dados no disco rígido, tornando as informações originais potencialmente irrecuperáveis e «abrindo a possibilidade da ocorrência de erros evitáveis em sede de investigação, que poderão pagar-se caro em julgamento»[218]. Tal justifica que o Ministério Público não deva demitir-se do seu papel de titular do inquérito.

Quando o investigador digital faz uso de um *malware* para obtenção de cópias do sistema operativo de um visado, haverá um incremento da complexidade refletido num necessário acréscimo de rigor na obediência de regras e princípios da Ciência Forense Digital.

Conforme ressaltado por James M. Aquilina, existe um processo nomeado de *evidence dynamics*, em que, muitas vezes, os investigadores digitais precisam de lidar com «qualquer influência que altera, realoca, obscurece ou oblitera evidências»[219], dado o facto de que o visado pela medida de intrusão, «poderá destruir propositalmente as evidências, excluindo *logs*, substituindo arquivos, ou encriptando dados incriminadores»[220].

São, portanto, necessárias informações prévias acerca do nível de sofisticação do visado para que o investigador possa antecipar a existência de exposição a perigos para o desempenho da sua função, na hipótese de o alvo da investigação ter conhecimentos informáticos, incluindo-se aí a capacidade de programação, inclusive para atender a eventual preocupação em manter o seu próprio endereço de IP oculto[221].

4.3. Medidas antiforenses: a criptografia, o projeto TOR e a esteganografia

Sendo o último propósito a construção de estruturas legais que possibilitem o uso de ferramentas como o código malicioso na recolha de fontes de meios de prova, tais pilares normativos precisarão de ser plenamente adaptáveis a ambientes reais, aptos a superarem tecnologias que visem dissimular ou ocultar elementos de interesse da investigação, conforme os exemplos adiante expostos.

---

[218]REAL, Rui Miguel dos Santos. «Apreensão, exame ou perícia e utilização processual de meios de prova existentes em material informático (documentos, correio electrónico, memorandos pessoais, fotografias, registos, áudio, etc). Enquadramento jurídico, prática e gestão processual.» *Meios de obtenção de prova e medidas cautelares e de polícia.* Lisboa: CEJ. 2019, p. 161 (Disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_MeiosProva.pdf; consultado pela última vez em 29/4/2021)

[219]AQUILINA, James M; CASEY, Eoghan; MAIL, Cameron H. *Malware Forensics: Investigating and analyzing malicious code.* Burlington: Syngress Publishing. 2008, p. xxvi

[220]Idem

[221]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 126 — 127.

Pode considerar-se que o argumento mais frequente na defesa do recurso a quaisquer métodos ocultos de investigação estatal em ambiente digital será a utilização cada vez mais disseminada de medidas antiforenses, constituindo-se na principal justificação para a implementação de uma legislação que autorize os órgãos de controlo a fazer uso de códigos arbitrários aptos a vigiar um arguido.

Os processos relacionados com a ciência forense digital necessitam de avaliar a possibilidade de os dados estarem armazenados em diversos locais dentro dos sistemas informáticos físicos e virtuais, na mesma medida em que devem equacionar a possibilidade de se encontrarem escondidos ou obliterados no seu interior.

O conceito mais transparente do objeto da presente análise é fornecido por Rui Miguel dos Santos Real, que esclarece que

> «a doutrina norte-americana convencionou chamar de medidas antiforenses, trata-se de um conceito abrangente, que inclui todos os métodos utilizados por agentes do crime para impedir ou obstaculizar a eventual investigação criminal dos ilícitos praticados pelos mesmos, aquando da prática do crime ou posteriormente, inutilizando a prova digital existente ou inviabilizando a sua análise por parte das autoridades estaduais».[222]

De ligação umbilical com o conceito exposto no tópico anterior, a base apresentada também sofre variação terminológica doutrinária, podendo tais métodos antiforenses ser caracterizados com um âmago comum a todas e quaisquer medidas ou ações que, nas palavras de Kevin Conlan, Ibrahim Baggile e Frank Breintige, possibilitem

> «enfatizar que medidas antiforenses podem ser identificadas por quaisquer tentativas de alterar, interromper, negar, ou, de alguma forma, interferir com procedimentos forenses de investigação cientificamente válidos»[223],

ressaltando que inclui também ferramentas não pensadas originalmente para esta finalidade.

Acerca das mencionadas funções e ferramentas não desenvolvidas *a priori* para se tornarem medidas antiforenses, esclarece-se que se darão num plano antecedente, se considerarmos o momento da investigação criminal e, mais precisamente, a atividade do

[222]REAL, Rui Miguel dos Santos. «Apreensão, exame ou perícia e utilização processual de meios de prova existentes em material informático (documentos, correio electrónico, memorandos pessoais, fotografias, registos, áudio, etc). Enquadramento jurídico, prática e gestão processual.» *Meios de obtenção de prova e medidas cautelares e de polícia.* Lisboa: CEJ. 2019, p. 162 (Disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_MeiosProva.pdf; consultado pela última vez em 29/4/2021)

[223]CONLAN, Kevin; BAGGILI, Ibrahim; BREITINGE, Frank. «Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy». *Digital Investigation*, Vol. 18. 2016, p. 567 (Disponível em: https://www.sciencedirect.com/science/article/pii/S1742287616300378; consultado pela última vez em 04/04/2021) (Tradução livre)

investigador digital que procederá à coleta de todas as provas e documentos disponíveis no sistema informático.

O autor do facto ilícito poderá preocupar-se em manter as suas ações e os rastos que as denotam distantes dos olhares das autoridades estatais, por meio de estratégias que frustrem a Ciência Forense Digital, que, por sua vez, serão compostas por táticas de *hardware* e *software*, aptas a travar o conhecimento do conteúdo de ficheiros e comunicações efetuadas.

A criptografia é o exemplo que demonstra plenamente esta particularidade e constitui uma ilustração acabada do quanto a vontade humana de manter informações sob segredo é preponderante ao longo da história. De acordo com Augusto Tavares Rosa Marcacini, «o primeiro livro impresso a abordar o tema intitula-se *Poligrafia*, publicado em 1510 por um abade alemão chamado Johannes Trithemius», que seria o primeiro teórico da face moderna desta disciplina[224].

O mesmo autor explica que a criptografia se constitui como um ramo dentro do estudo da criptologia, o que a coloca no campo das Ciências Exatas, pelo recurso a um algoritmo matemático para tornar um texto ilegível, podendo ser descrita como «a arte de escrever em cifra ou em código»[225].

Seguindo os ensinamentos do referido jurista, assinala-se que a técnica pode ser tão simples como a criptografia de chave simétrica, usada desde que a palavra escrita se configurou como meio comum para enviar mensagens em tempos de guerra, quando o remetente e destinatário conheciam a senha para decifrar a mensagem. Já na criptografia de chave assimétrica, proposta somente a partir de 1976 e de utilização abrangente em aplicações da Internet nos dias atuais, haverá uma chave pública conhecida pela generalidade dos utilizadores de um *software* e uma segunda chave privada, calculada por computador e de conhecimento exclusivo do utilizador[226].

A criptografia de dados, aliada à capacidade computacional, permite ao seu usufruidor proteger um sistema informático inteiro, um conjunto de dados em transmissão ou um único ficheiro num código criptográfico, o que torna o acesso ao conteúdo em texto simples praticamente inviável para quem não tenha a respetiva chave para desencriptação, inviabilizando, assim, o conhecimento do conteúdo para terceiros.

[224]MARCACINI, A. T. *Direito e Informática: uma abordagem jurídica sobre a criptografia.* São Paulo: Editora Forense, 2002, p. 20
[225]Idem, p. 19
[226]MARCACINI, A. T. *Direito e Informática: uma abordagem jurídica sobre a criptografia.* São Paulo: Editora Forense, 2002, p. 26 — 31

Como destaca Orin S. Keer[227], na tentativa de revelar o conteúdo cifrado, um único computador poderá demorar milhares de anos até encontrar uma única chave criptográfica. Observando o cenário, é possível constatar que constitui uma ferramenta definitivamente poderosa e um dos avanços mais expressivos dos últimos anos, com a capacidade de frear o poder punitivo.

Este facto pode ser demonstrado ao verificar que o FBI, apenas no ano de 2017, deixou de efetivar o acesso a 7800 dispositivos móveis, não obstante existirem decisões judiciais que facultam o ingresso ao interior dos citados processadores de dados. Tal circunstância levou o procurador-geral adjunto e o diretor-geral do FBI a emitirem opiniões no sentido de que deveria ser criada uma regulamentação legal para a questão da encriptação, fornecendo ao Estado a possibilidade de acesso a chaves que facultariam o ingresso ao sistema informático ou ao texto simples[228].

Caso a metodologia adotada para conceder acesso a dispositivos e ficheiros encriptados por órgãos de controlo seja a instalação de *backdoors* na generalidade dos aparelhos, levantar-se-ão inevitavelmente questões acerca da facilidade criada para intrusão também por pessoas mal-intencionadas.

Um exemplo que ficou conhecido acerca das dificuldades com as quais se deparam os órgãos de controlo, na tentativa de aplicar a lei, sempre que procurem provas contidas em dispositivos ou discos rígidos completamente encriptados, materializou-se na disputa judicial em que figuraram, de um lado, o FBI e, no polo oposto, a empresa Apple. A disputa consistia na demanda policial com a finalidade de obter ordem judicial determinando que a empresa prestasse auxílio no acesso ao conteúdo de um iPhone 5C, propriedade do condado de San Bernardino, no estado norte-americano da Califórnia. Tal dispositivo necessitava de ser analisado em decorrência da investigação de um massacre em território norte-americano, ocorrido no mês de dezembro de 2015, por pertencer a um dos atiradores que falecera naquela data. O telemóvel encontrava-se

[227]KERR, Orin S. «The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"». *Connecticut Law Review,* Vol. 33. 2001, p. 503. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=927973, consultado pela última vez em 04/10/20)

[228]PFEFFERKORN, Riana. *The Risks of "Responsible Encryption".* The Center for Internet and Society. 2018, p. 2 – 3 (Disponível em: http://cyberlaw.stanford.edu/files/publication/files/20 18-02-05%20Technical%20Response%20to%20Rosenstein-Wray%20FINAL.pdf, consultado pela última vez em 25/03/2021)

> «bloqueado com uma senha de quatro dígitos, dificultando o processo de aquisição forense devido às técnicas anti-forenses integradas que reforçam a criptografia e a limpeza automática do dispositivo após várias tentativas sem sucesso de senha»[229].

Conscientes de que o litígio poderia vir a ser prolongado, a solução encontrada pelos agentes de polícia foi a aquisição do conteúdo do dispositivo por meio de um «*exploit* de dia zero»[230]. Segundo os ensinamentos de Juliana Campos, um «*exploit* de dia zero» é

> «uma vulnerabilidade que seja desconhecida pelos produtores (portanto, não corrigida), pois desse modo poderão concretizar o ataque que pretendem com maior eficácia. Estas vulnerabilidades (desconhecidas e não corrigidas) denominam-se 'vulnerabilidades de dia-zero' ('*vulnerabilities zero-day'*) referindo-se ao número de dias desde a sua descoberta, por contraposição às 'vulnerabilidades de dia-n' ('*vulnerabilities n-days'*), que são conhecidas e para as quais não existe uma correção ('*patch'*) ou existindo esta última, o sistema que se pretende atingir não procedeu à atualização que a corrigiria»[231].

O panorama aqui descrito demonstra que uma das únicas medidas eficazes para aceder ao conteúdo cifrado será, de facto, o *malware,* já que a implementação coativa de *backdoors* em produtos de *hardware* e *software* fragiliza demasiado a privacidade, inclusivamente aquela que é necessária ao próprio Estado. Deve considerar-se ainda que a revelação forçada de senha para desencriptação estaria vedada pelo princípio do *nemo tenetur se ipsum accusare,* consubstanciado no disposto no art.º 14.º, n.º 5, da Lei do Cibercrime[232].

Não apenas os infratores contumazes, mas também indivíduos residentes em países que se encontrem sob regimes ditatoriais repressivos podem desejar manter-se anónimos enquanto utilizam a *Internet*. Isto tende a impedir uma identificação e deteção do processador de dados de onde partiram as requisições para ingresso em páginas *Web* com conteúdo de doutrinação terrorista ou destinadas à inserção e visualização de fotografias pedopornográficas, por exemplo.

Tal navegação ocorre, por regra, numa área da Internet conhecida por *Deep Web,* onde os navegadores mais utilizados (*Safari, Firefox, Chrome*) não permitem o acesso à estrutura

[229]CONLAN, Kevin; BAGGILI, Ibrahim; BREITINGE, Frank. «Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy». *Digital Investigation*, Vol. 18. 2016; p. 67 e 68 (Disponível em: https://www.sciencedirect.com/science/article/pii/S1742287616300378; consultado pela última vez em 25/03/2021) (Tradução livre)
[230]Idem
[231]CAMPOS, Juliana. *O Malware como Meio de Obtenção da Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 16 (Versão eletrónica)
[232]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 54, p. 169 — 170

diferenciada das URL (*Uniform Resource Locator*) hospedadas[233]. Este conceito é contraposto ao da conhecida *Surface Web*, consistente em páginas *Web* selecionadas e acessíveis através de motores de pesquisa como o *Google*, *Bing ou Yahoo!*[234].

A navegação anónima cria obstáculos que dificultam ao agente estatal associar o crime ao seu perpetrador, impedindo a identificação do verdadeiro número IP responsável pela conduta delituosa. Para esta finalidade, o utilizador pode lançar mão de servidores *proxy*, um dispositivo ou um *software* que atua em nome dos seus clientes, intermediando as requisições oriundas dos mesmos, oportunidade em que o servidor que hospeda uma eventual página *Web* de conteúdo criminoso receberá somente o número IP do servidor *proxy*, jamais o do real destinatário do conteúdo[235].

Porém, esta tática não será completamente segura, já que tais servidores *proxy* podem armazenar as informações acerca dos pedidos de acesso a páginas *Web*, repassando-as ao investigador digital. Mesmo que diversos servidores *proxy* sejam usados em cadeia (*mix cascades*), o risco de identificação permanecerá[236].

Deste modo, apesar de a doutrina referir a existência de outros *softwares* que possuem a função de fornecer uma navegação incógnita, como por exemplo o *Freenet*, o recurso mais difundido e aparentemente mais funcional para a anonimização completa durante a interação *on-line* será o programa TOR (*The Onion Router*). Desenvolvido pela Marinha dos EUA para estabelecer comunicações militares no final da década de noventa, o *software* veio a conhecimento público no ano de 2004[237].

O TOR é constituído por uma infraestrutura que, além de impossibilitar o conhecimento das mensagens enviadas, bloqueia a análise de tráfego na rede. Figurativamente, a imagem mais didática para explicar o funcionamento do programa foi definida por meio de uma descrição elaborada por Nilesh Patil, em uma comparação com uma realidade do mundo físico.

Esta imagem sublinha a ideia de um quarto fechado, com inúmeras pessoas no seu interior e, a dado momento, é entregue a qualquer dos ocupantes do recinto um cilindro com

[233]ORTIZ PRADILLO, Juan Carlos. «Fraude y anonimato en la red: cuestiones constitucionales y procesales de la desanonimización de la red TOR». AA.VV. C. S. Crespo, Fraude Electrónico – *Su gestión penal y civil.* Valência: Tirant to Blanch. 2015, p. 46 — 47 (Versão eletrónica)
[234]RAMALHO, David Silva. «A investigação criminal na Dark Web». *Revista de Concorrência e Regulação,* Ano IV, n.º 14/15. Abr. — set. 2013, p. 385
[235]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 153 — 154
[236]Idem
[237]RAMALHO, David Silva. «A investigação criminal na Dark Web». *Revista de Concorrência e Regulação,* Ano IV, n.º 14/15. Abr. — set. 2013, p. 387 – 390

várias camadas de papel e com o nome deste escrito na camada mais externa. Ao receber o cilindro, o recetor ouviu do mensageiro a informação de que deverá arrancar esta camada mais exterior onde existe seu próprio nome escrito e, assim, revelar o nome constante da camada seguinte. É justamente esta pessoa que terá o nome revelado, aquele que virá a ser o próximo destinatário para quem o nosso recetor originário deverá passar o cilindro. O novo destinatário repetirá a instrução e assim sucessivamente, até que o cilindro chegue ao recetor final[238].

Na analogia acima descrita, cada mão pela qual o cilindro passa corresponde a um nó da rede TOR, composta por voluntários que podem disponibilizar parte da largura da sua banda[239], funcionando como «retransmissores de comunicações»[240]. O cilindro constitui a mensagem em si, enviada com várias camadas de criptografia, semelhantes às camadas de uma cebola, de modo que, após sair do último nó para o computador do destinatário final, a última camada de criptografia é retirada, revelando o conteúdo da mensagem e fazendo com que nenhum observador externo consiga seguir o percurso aleatório que a mensagem fez desde a sua saída até à sua efetiva entrega.

O TOR possibilita ainda o desenvolvimento de *sites* na Internet chamados *hidden services*, que operam por forma a ocultar o endereço IP dos servidores que os hospedam, sendo acessíveis apenas através do *Tor Browser*[241].

Fica, assim, possibilitada a instalação de *software* malicioso nestes sítios eletrónicos, para subsequente infeção involuntária pelo programa espião no equipamento de todos aqueles que ingressem em tais *websites*, indivíduos que até então ostentam a condição de indeterminados.

Outra técnica que pode ser utilizada por transgressores com o intuito de esconder a existência de ficheiros de áudio, fotos e vídeos é conhecida como esteganografia. Mais uma vez, é uma técnica utilizada há séculos, constando que o primeiro livro escrito sobre o tema veio a lume na Grécia, no ano de 1600, com o título *Steganographica*, através da pena de Gaspari Schotti[242].

---

[238]PATIL, Nilesh; LINGAM, Chelpa. «Anonymous connections and onion routing». *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, n.º 2. Fevereiro de 2012, p. 1 – 2

[239]ORTIZ PRADILLO, Juan Carlos. «Fraude y anonimato en la red: cuestiones constitucionales y procesales de la desanonimización de la red TOR». AA.VV. C. S. Crespo, Fraude Electrónico – *Su gestión penal y civil.* Valência: Tirant to Blanch. 2015, p. 51 (Versão eletrónica)

[240]RAMALHO, David Silva. «A investigação criminal na Dark Web». *Revista de Concorrência e Regulação,* Ano IV, n.º 14/15. Abr. — set. 2013, p. 391

[241]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 156 — 157

[242]SHINDER, Debra Littlejonh. *Scene of the Cybercrime: Computer Forensics Handbook.* Massachusetts: Syngress. 2002, p. 384

Podendo ser comparada com a escrita em papel usando uma tinta mágica que desaparece quando seca, este método proliferou por meio da Internet, existindo, atualmente, centenas de programas com esta finalidade espalhados por páginas da *Web*[243].

Um programa de esteganografia possibilita que um utilizador recorra a qualquer ficheiro como «vetor para transportar os dados ocultos»[244]. A título de exemplo, referem-se os ficheiros aparentemente inócuos com extensões como .pdf ou .jpg. A informação oculta compõe uma carga útil introduzida no ficheiro através de um processo criptográfico, que o torna, regra geral, invisível a olho nu e obriga o especialista a procurar todos os programas desta natureza no sistema informático.

[243]HOMSTER, Chet. «Discovery Hidden Evidence». *Journal of Digital Forensics Practice*, Vol. 1, n.º 1. 2006, p. 47 — 48
[244]Idem, p. 48

5. REQUISITOS PARA CONSTRUÇÃO DE UM REGIME JURÍDICO QUE POSSIBILITE O USO DA TÉCNICA DE *MALWARE* EM INVESTIGAÇÕES CRIMINAIS

5.1. A inadmissibilidade do uso da técnica de *malware* em investigações criminais em Portugal

Nos dias de hoje, os métodos de obtenção de provas digitais estão regulamentados em Portugal por meio do Código de Processo Penal, pela Lei n.º 32/2008, de 17 de julho (relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações) e, primordialmente, pela Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime). A doutrina acusa a multiplicidade de ordenamentos de causar falta de clareza, indicando que um regime jurídico único para tratar a matéria resultaria em benefícios operacionais para os juristas e segurança para a sociedade.

Como João Conde Correia afirma, existem três diplomas para regulamentar partes de uma única e íntegra realidade. Esta tríade

> «para além de acentuar o atual paradigma da descodificação e de negar a desejável centralidade normativa do Código de Processo Penal, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático»[245].

O investigador defende e antecipa que, de entre todos aqueles métodos referidos como já previstos na lei, não se antevê uma pormenorização ou uma precisão suficientes que permitam denotar a autorização para o uso de *software* malicioso, sob qualquer interpretação que considere a primazia da CRP sobre o ordenamento[246].

O código arbitrário tem a aptidão para aceder a todo o conteúdo armazenado, aproximando-se das já habituais buscas e apreensões materiais do *hardware* dos computadores. Os investigadores forenses anunciam, assim, a sua presença física ao suspeito ou arguido e, por via de consequência, a própria existência de uma investigação, para explorarem *a posteriori* as informações existentes na memória do dispositivo.

Consoante os ensinamentos de Juliana Campos, esta última hipótese não está, no entanto, abrigada pela previsão constante do art.º 174.º do CPP para efeito de conceder

[245]CORREIA, João Conde. «Prova digital: as leis que temos e as leis que deveríamos ter», *Revista do Ministério Público*, n.º 139. Julho — setembro de 2014, p. 30

[246] CAMPOS, Juliana. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 40 (versão eletrónica)

judicialmente uma «busca *on-line*» à distância e efetivada por um código arbitrário, já que, por se tratar de dados digitais, a matéria seria pertencente à delimitação de uma temática constante do âmbito da Lei n.º 109/2009, de 15 de setembro[247].

Uma vez que a arquitetura delineada pelo legislador necessitará de traçar a distinção entre a captura de dados armazenados e aqueles produzidos em tempo real, distinguindo, de entre estes últimos, os internos e externos ao sistema informático, torna-se indispensável observar que o deferimento de todas estas possibilidades de extração de dados em conjunto pode recair num limite impeditivo de utilização prática, pela capacidade de patrulhamento total, formadora de um perfil personalíssimo e absoluto do visado[248].

Exemplifica-se superficialmente, a partir deste ponto, aqueles métodos que nos fornecem pistas dos requisitos que devem ser eleitos como indispensáveis para a efetiva regulamentação do *software* malicioso como ferramenta policial na obtenção de fontes de prova.

Os primórdios do instituto da intercetação telefónica datam de uma época em que os desafios do mundo virtual eram inexistentes ou extremamente escassos. Contudo, este é o método de obtenção de prova oculto e à distância com o qual a comunidade de jurisconsultos está mais familiarizada. Está, inclusivamente, demonstrado na regulamentação das escutas alguns requisitos jurídicos indispensáveis genericamente a todos os artifícios que operem de modo similar.

A experiência em Portugal faz com que as escutas telefónicas sejam uma medida facultada em processo criminal pelo art.º 34.º, n.º 4, da CRP, considerada pelo legislador já como última alternativa a ser deferida quando for indispensável ao descobrimento da verdade ou quando, de outro modo, não for exequível adquirir a prova. Nem sempre é simples para o magistrado judicial aferir isto, de modo que os pedidos oriundos dos membros do Ministério Público devem conter a justificação comparativa de todas as alternativas viáveis para a descoberta da verdade.

Foi vontade do legislador que a intercetação telefónica fosse utilizada apenas na fase de persecução para repressão criminal, não sendo viável o seu deferimento na prevenção dos crimes que possam ocorrer difusamente ou que não estejam sequer em fase de planeamento.

[247]CAMPOS, Juliana. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 40 (versão eletrónica)
[248]ALBUQUERQUE, Paulo Pinto de. *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*. Lisboa, Universidade Católica. Ed. 2011, p. 332 — 333

Naturalmente, a cognição judicial está limitada ao pedido do MP, que pode ser indeferido no todo ou em parte, jamais ultrapassado no sentido de uma decisão *extra* ou *ultra petita*.

O juiz está adstrito à verificação de indícios da existência de um crime constante de um catálogo taxativo, podendo admitir a medida contra o arguido ou suspeito, contra quem funcione como retransmissor de mensagens e, ainda, a gravação de comunicações da vítima, caso esta dê o seu consentimento. Seguindo o posicionamento de Lydie Jorge Batista, os sujeitos que vierem a sofrer esta restrição deverão ser «pessoas concretas e determinadas»[249].

O CPP, no seu art.º 187.º, n.º 6, limita o prazo de autorização da medida a três meses, renovável por iguais períodos, não devendo, contudo, ultrapassar o prazo a que está sujeita a própria investigação policial preliminar.

O diploma processual penal português inclui, no seu art.º 189.º, a possibilidade de estender a interferência e gravação de comunicações desenvolvidas por meios técnicos diferentes do telefone, especificamente através do correio eletrónico e da transmissão de dados por via telemática.

Caso seja corretamente analisado, o contexto do artigo anunciado faz com que o programa arbitrário permaneça como aparato atípico, já que a interceção de comunicações não se confunde com o *malware.* Este, por sua vez, possui capacidades muito superiores já devidamente explicadas, permitindo, inclusivamente, o conhecimento de processos não comunicacionais, como é exemplo o caso dos dados de localização obtidos por meio de GPS[250].

O investigador reforça a doutrina adotada por Juliana Campos, já que, ao comparar a intercetação telefónica com um regime que venha a estabelecer o uso da ferramenta de código arbitrário, ambos serão

> «materialmente distintos, pelo que, em princípio, deverá ser mais apertado o núcleo de crimes em [que] se admite a utilização de *malware* quando comparado com outros meios de obtenção da prova que revelam um menor grau de lesividade dos direitos já consagrados»[251].

A localização celular é uma medida prevista no art.º 252.º-A do Código de Processo Penal, constituindo-se na possibilidade de identificação territorial mais ou menos precisa[252]

[249]BATISTA, Lydie Jorge. *O Malware como Meio de Obtenção de Prova em Processo Penal.* Dissertação de Mestrado em Ciências Jurídico-Forenses. Faculdade de Direito – Universidade de Lisboa. 2018, p. 99
[250]BRITO, Maria Beatriz Seabra de. *Novas Tecnologias e Legalidade da Prova em Processo Penal*. Coimbra: Almedina. 2018, p. 91
[251]CAMPOS, Juliana. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 82 (versão eletrónica)
[252]SILVA, Ricardo Sidi Machado da. *A Interceptação das Comunicações Telemáticas no Processo Penal*. Dissertação de Mestrado em Direito Processual. Faculdade de Direito – Universidade de São Paulo. 2014, p.

de um dispositivo em conexão com os aparelhos de propriedade das operadoras de telefonia móvel, por uma constante troca de sinais que ocorre entre os nossos utensílios eletrónico-digitais e as antenas mais próximas.

A autorização contida neste preceito não pode jamais significar qualquer hipótese de permissão para a invasão remota de um equipamento eletrónico-digital com a finalidade de obter informações transmitidas a partir do GPS embutido. A natureza do conhecimento que se consegue alcançar nesta circunstância é diferente, no que à precisão diz respeito, já que tais dados são produzidos devido à efetivação de uma triangulação da posição do equipamento via satélite[253].

A Lei do Cibercrime prevê, no seu art.º 15.º, n.º 1, que a autoridade judiciária pode ordenar pesquisas por «dados informáticos específicos e determinados», em sistemas individualizados, presidindo a diligência. O sentido deste preceito legal é complementado pelo n.º 5 do mesmo artigo, que prevê a extensão da determinação para pesquisa, sempre que os dados procurados estejam «noutro sistema informático, ou numa parte diferente do sistema pesquisado», desde que legitimamente acessíveis a partir do primeiro.

A única interpretação viável neste caso condiz com uma pesquisa efetuada após a realização de uma busca e apreensão do *hardware* de um equipamento eletrónico-digital, já que a anunciada necessidade de a autoridade judiciária presidir a diligência no momento da sua efetivação entrará em contradição direta com o secretismo que se possa desejar atribuir à medida[254].

A previsão do art.º 15.º, n.º 5, da Lei n.º 109/2009, de 15 de setembro, poderá ser aplicada, caso o especialista informático que execute a pesquisa no sistema originário venha a perceber que as informações desejadas se encontram, na realidade, numa conta de *e-mail* ou num serviço de armazenamento em nuvem. Por exemplo, se já possuem as credenciais de *log* e senha inseridas e guardadas na memória do equipamento apreendido fisicamente.

Como é possível prever, não se encontra em larga escala a defesa de uma posição que transpareça e aceite qualquer possibilidade de autorização para apreensão de dados informáticos remotamente por meio de *software* malicioso intrusivo no n.º 7 do art.º 16.º da

66, disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-04032015-082717/publico/Ricardo_Sidi_Dissertacao_Mestrado_Integral.pdf, consultado pela última vez em 06.03.2012, que identifica que no Brasil há uma baixa precisão da localização do usuário, a ponto de se concluir que poderia não ser útil para a efetuar prisão em flagrante delito após o cometimento de um crime

[253]BRITO, Maria Beatriz Seabra de. *Novas Tecnologias e Legalidade da Prova em Processo Penal*. Coimbra: Almedina. 2018; p. 88

[254]CORREIA, João Conde. «Prova digital: as leis que temos e as leis que deveríamos ter», *Revista do Ministério Público*, n.º 139. Julho — setembro de 2014, p. 42.

Lei do Cibercrime, já que o dispositivo tem uma vocação clara para delinear procedimentos consistentes ou imediatamente posteriores a uma apreensão palpável.

Como mecanismo de obtenção de provas digitais, o art.º 18.º do diploma em questão permite a interceção, durante o processo comunicativo, daqueles dados que entram e saem do equipamento eletrónico-digital, havendo passado anteriormente por um provedor de serviços, como, sem dúvida, se verifica em relação aos dados de tráfego.

Assim, a exemplo do que se passa nas intercetações e gravações telefónicas de um determinado número publicamente disponibilizadas pela operadora de serviços, o dispositivo em questão autoriza somente os provedores e servidores de *Internet* a facultar o conhecimento daquilo que passou pelos seus próprios sistemas durante determinado período.

Os dados facultados aos órgãos de controlo do Estado serão o conjunto de *bits* que compõem os pacotes de dados que trafegam pela rede, entrando ou saindo de um sistema informático da posse do visado, individualizado pelo número IP e pelos demais dados de base.

O *software* malicioso, conforme explicado, não capta apenas os processos de comunicação, sendo indefensável a instalação deste para apreensão apenas de trocas comunicativas[255].

Assim, o investigador sustenta que as autoridades de segurança e judiciárias poderiam dispor de ferramentas de natureza *packet sniffer* com a finalidade exclusiva de rastrear em tempo real o movimento de dados na rede, já que as mencionadas autoridades devem permanecer atentas ao menor nível de prejuízo possível para os visados no decurso das atividades de recolha de dados.

Na busca pela legitimidade da ação do juízo criminal que venha dispor de determinado código arbitrário para o apuramento da verdade, chega-se ao ponto que diz respeito ao instituto das ações encobertas em ambiente virtual. Apenas se menciona a sua correlata definição de agente encoberto, sem perder de vista a combinação com o distinto conceito de agente provocador, o que nos reconduz ao regime geral imposto pela Lei 101/2001.

É possível encontrar na especificação dada pelo n.º 2 do art.º 19.º, da Lei 109/2009, de 15 de setembro, a previsão de que «sendo necessário o recurso a meios e dispositivos informáticos, observa-se, naquilo que for aplicável, as regras previstas para a interceção de

[255]CAMPOS, Juliana. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 42 (versão eletrónica)

comunicações», para fins exclusivos de persecução e repressão penal[256]. Não carece de defesa doutrinária o posicionamento de que o código malicioso está, nesta formulação, devidamente tipificado[257] para o contexto das ações encobertas.

Sem embargo, David Silva Ramalho defende que a expressão «meios e dispositivos informáticos» consagra, naquela norma, uma autorização para o uso das técnicas de *hacking*[258] e a instalação de *malware*, que «devam ser utilizados quando a própria acção encoberta e os demais métodos ocultos forem incapazes de dar respostas às exigências da investigação»[259], compreendendo, ainda, que inexiste mecanismo paralelo no ordenamento para servir de parâmetro.

Conquanto que se adota a linha defendida por Lydie Jorge, observam-se os seus argumentos expendidos apontando para a ausência de acatamento aos princípios de reserva de lei e densidade legal, tudo a indicar que a verdadeira intenção do legislador foi apenas facultar ao agente que esteja a atuar de modo encoberto, uma participação em fóruns *on-line*, ainda que privados, receção e envio de material contendo pedopornografia e outras ações semelhantes em ambiente virtual, para efeitos de ganhar a confiança de um ou vários suspeitos de crime[260].

Por seu turno, Juliana Campos ressalta que

> «o *malware* e as ações encobertas em ambiente digital não se confundem, desde logo atendendo à sua natureza, ou seja, o primeiro é um *software* que é instalado e recolhe prova *motu proprio*, ao passo que nas segundas se está perante funcionários de investigação criminal ou terceiros»[261].

5.2. A inadmissibilidade do uso da técnica de *malware* em investigações criminais no Brasil

O histórico de produção legislativa acerca do tema da intercetação de comunicações telefónicas na República Federativa do Brasil de 1988 sofreu de um determinado atraso,

[256]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Edições Almedina. 2017, p. 347
[257]RAMALHO, David Silva. «O Uso de *Malware* como Meio de Obtenção de Prova em Processo Penal». *Revista de Concorrência e Regulação*, Ano IV, n.º 16. Out. — dez. de 2013, p. 231 — 233
[258]David Silva Ramalho refere que «o termo *hacking* significa, em sentido amplo a utilização de um sistema informático com o intuito de obter acesso não autorizado a outro(s) sistema(s) ou ficheiro(s)», (RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 318)
[259]RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina. 2017, p. 346
[260]BATISTA, Lydie Jorge. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Dissertação de Mestrado em Ciências Jurídico-Forenses. Faculdade de Direito – Universidade de Lisboa. 2018, p.129 — 130
[261]CAMPOS, Juliana. *O Malware como Meio de Obtenção de Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 42 (versão eletrónica)

refletindo a existência e o uso deste meio oculto de obtenção de fonte de prova antes mesmo da plenitude da sua legitimidade.

Ao longo do presente estudo, observa-se que qualquer meio oculto de obtenção de fontes de prova deve seguir o preceito da reserva legislativa como condição indispensável para efetivar a restrição de direitos fundamentais, sempre na menor intensidade possível. Tratando aqui da legitimação de utilização de códigos arbitrários em fase pré-processual, não é cabível a aplicação subsidiária do Código de Processo Civil, no seu art.º n.º 369.º, que prevê a irrestrita legalidade de provas moralmente legítimas.

Observa-se que a visão restritiva do que é uma prova atípica é largamente aceite no Brasil, quando, na verdade, além da autorização genérica para a adoção de um método oculto de obtenção de fontes de prova, a lei precisa igualmente de regular os procedimentos pertinentes[262]. Eventualmente, o legislador desta nação terá permanecido inerte desde outubro de 1988, quando a redação do art.º 5.º, inciso XII, CRFB/88, autorizou a restrição ao sigilo das comunicações telefónicas.

Sem ingressar na dúbia redação do dispositivo constitucional, a inação legislativa veio somente a termo no dia 24 de julho de 1996, com a publicação da Lei n.º 9296, para a qual o investigador olha de modo necessariamente lacunar.

No interregno entre a vigência da constituição e da norma infraconstitucional, a circunstância de tempo acarretou a declaração de nulidade de inúmeras decisões judiciais que facultavam a intercetação e gravação das ligações telefónicas.

Tais decisões deferindo os pedidos de intercetação telefónica foram originalmente registadas com base no Código Brasileiro de Telecomunicações (Lei n.º 4197/42). Assim que a matéria aportou nos tribunais superiores[263], levantou-se a discussão acerca da receção deste dispositivo de base e, por fim, reconheceram que a atipicidade era um entrave para a concessão do uso deste método de obtenção de fonte de prova. Isto é, a Carta Magna de 1988 consagrou a norma que facultava o uso de gravações telefónicas com uma eficácia limitada, passível de aplicação apenas após a regulamentação advinda do legislador ordinário.

Conforme consta do parágrafo único do art.º 1.º da Lei n.º 9296/96, o legislador estendeu o mesmo regime jurídico para a «intercetação do fluxo de comunicações em

[262]SILVA, Ricardo Sidi Machado da. *A Interceptação das Comunicações Telemáticas no Processo Penal*. Dissertação de Mestrado em Direito Processual. Faculdade de Direito – Universidade de São Paulo. 2014, p. 171

[263]Brasil. Supremo Tribunal Federal. HC69.912-0/RS, Pleno, Rel. Min. Sepúlveda Pertence, Julgado em 16.12.1993, DJ 25.05.1994

sistemas de informática e telemática». Ficou exposto que nem a mais branda intercetação telemática seria permitida durante a investigação de crimes punidos com pena de reclusão.

A concessão da medida possui natureza cautelar, exigindo a presença de «indícios razoáveis de autoria ou participação em infração penal», e a observância da subsidiariedade, sem que possa subsistir como primeiro ato de investigação. O legislador absteve-se de elencar um rol taxativo de crimes, que pudesse vincular o ensejo da aquiescência ao pedido feito pela Polícia Judiciária ou pelo Ministério Público.

A vocação da norma abrange, assim como em Portugal, a comunicação ocorrida no mesmo instante em que for captada, excluindo qualquer dado em repouso no interior do sistema informático, não abrangendo a intrusão de um *malware*, já que este tipo de *software*, que pode fornecer um *backdoor*, aumenta a dificuldade de segurança para todos os utilizadores.

O regime da mencionada lei estabelece que o prazo será concedido até um máximo de quinze dias, renováveis por igual período, nos termos do seu art.º 5.º. Conforme sufragado pelos tribunais superiores, não há limite para renovação desta mesma dilação, o que na prática permite a sua constância enquanto perdurarem as razões da sua concessão.

Caso seja implantado, por exemplo, um *software* malicioso para a atividade de vigilância, seria relevante que a decisão judicial viesse a estabelecer previamente o início para a vigência de contagem de prazo, a denotar contribuição para razoabilidade.

Esta hipótese só é sugerida para antecipar que o *malware* já foi instrumento utilizado no âmbito de investigações efetuadas de modo apartado das fronteiras da tipicidade, concretizadas pela Polícia Federal do Brasil sob a supervisão direta do Ministério Público Federal.

Tal evento decorreu durante a denominada operação *darknet*[264], que atuou no âmbito da investigação e consequente prisão de suspeitos, entre o final do ano de 2013 e 2016, ano em que esta operação foi concluída.

O relato oficial deixa transparecer que os órgãos de controlo suspeitavam de que o tipo constitutivo do crime previsto no art.º 241.º-A do Estatuto da Criança e Adolescente[265] estava a ser alvo de transgressão. As imagens de «registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente» estariam a ser distribuídas na *deep web*, a partir da rede TOR.

[264]Conforme informação constante do sítio eletrónico oficial do Ministério Público Federal disponível em www.mpf.mp.br/rs/sala-de-imprensa/docs/outros-documentos/operacao-darknet.
[265]Disponível em: www.planalto.gov.br/ccivil_03/leis/l8069.htm.

Para obter o número de IP dos sistemas informáticos utilizados para a execução dos delitos, foi desenvolvido pela própria Polícia Federal aquilo que foi designado simplesmente por «ferramenta». Era um *malware* que, possivelmente, infetou os sítios eletrónicos nos quais se encontravam hospedadas as tais imagens e os fóruns de conversação utilizados pelos infratores, para se infiltrar sequencialmente nos equipamentos eletrónico-digitais destes.

Em seguida, após obter, por via de consequência, a individualização dos suspeitos, a operação declinou a competência para os diversos juízes federais, que, nas respetivas subsecções judiciárias, ordenaram o cumprimento de dezenas de mandados de captura e outras tantas buscas e apreensões físicas dos sistemas informáticos.

São poucos os pormenores que se tornam públicos neste tipo de operação extremamente secreta, com especial relevo ao cariz oculto atribuído à ferramenta desenvolvida pela equipa das forças de segurança e as potencialidades utilizadas no curso da mesma. A legislação de base para fundamentar o pedido de infiltração do *malware* estatal correspondeu ao art.º 10.º da Lei 12 850, datada de 12 de agosto de 2013, cujo escopo consiste na definição de organização criminosa e dispor sobre a investigação criminal os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal.

A redação do artigo de lei, não obstante, prevê apenas a existência do agente de polícia infiltrado em organizações criminosas, sem jamais estabelecer a possibilidade de uso de código arbitrário ou regulamentar a sua atividade como investigador no ambiente virtual.

A formulação gramatical exposta pela lei informa que a mesma está voltada para «a infiltração de agentes de polícia em tarefas de investigação», não autorizando qualquer confusão entre um agente de polícia e o código malicioso, já que todo o texto foi direcionado para o combate a crimes no mundo físico. Autoriza apenas uma atuação que esconda a sua função policial e consequente ocultação de sua real identidade, ganhando a confiança no seio de uma organização voltada ao cometimento de delitos.

5.3. Requisitos materiais, formais e orgânicos

No momento em que o legislador de Portugal e o do Brasil resolverem que a indeterminação atual quanto ao tema não será mais considerada tolerável, será necessário formular uma legislação que atenda ao princípio da determinabilidade e precisão dos atos normativos. Deverá levar em consideração, deste modo, o respeito ao critério formal, já que, tratando-se de um instrumento que permite investigação estatal oculta e abrangente, será imprescindível que os seus destinatários possuam a noção das circunstâncias em que será possível esperar uma intervenção desta natureza.

Como regra, a ferramenta que será utilizada no curso do inquérito levado a cabo pela polícia deverá atender também aos requisitos materiais, considerando que, no momento anterior ao processo penal, os direitos fundamentais do arguido encontram menor guarita[266].

Para o instante da decisão judicial de concessão da medida, a lei não poderá requerer a presença de qualquer elemento indistintamente como base para tanto. Ter-se-á de exigir a presença de fortes indícios, a revelar a probabilidade de cometimento da infração, já que permite um grau de intrusão imensamente superior, por exemplo, ao das escutas telefónicas.

Importa ressaltar que, se, para deferimento de uma escuta telefónica, o legislador já determinou que deveriam existir indícios suficientes de autoria e materialidade para que só assim o magistrado judicial pudesse conceder a interceção, parece natural que, para uma intervenção superior, as exigências sejam igualmente mais apertadas.

Prosseguindo no paralelo estabelecido com as escutas telefónicas, a nova lei apenas poderá facultar o uso do aparato em face do arguido, daquele que funcione como retransmissor de mensagens para este, ou da vítima, sempre que haja consentimento da mesma para a implementação do código malicioso no seu sistema informático.

Os métodos ocultos de investigação criminal efetivados à distância não têm autorização nos ordenamentos de Portugal e do Brasil para fins preventivos. Não poderão, igualmente, ser direcionados a uma coletividade indeterminada de pessoas, e afigura-se inviável a instalação do *malware* em *websites* ou endereços de *e-mail* para fins de individualização de um suspeito, já que possuem o potencial de atingir um número indeterminado de indivíduos.

Outro dever do legislador será evitar quaisquer dubiedades. Deverá, portanto, referir expressamente que se trata da infiltração de programa informático malicioso, adotar categoricamente a nomenclatura *malware* e especificar, rigorosamente, as funcionalidades eleitas como permitidas para ativação num cenário de investigação policial.

Assim, o legislador decidirá se faculta o acesso remoto *on-line* aos dados em repouso na memória do dispositivo eletrónico-digital e se os dados produzidos em tempo real (conhecidos na Alemanha como «vigilância na fonte») deverão ser remetidos, por esta via, aos investigadores.

[266]CAMPOS, Juliana. *O Malware cromo Meio de Obtenção de Prova em Processo Penal*. Coimbra: Edições Almedina. 2021, p. 82 (versão eletrónica)

Sob este aspeto, escolherá se as imagens e os sons[267] existentes em redor do equipamento infetado poderão ser captados por meio de comandos transmitidos ao *hardware*, destacando-se, neste ponto, a previsão quanto ao local em que podem ser implementadas: se dentro ou fora do domicílio.

Para garantia do princípio do devido processo legal, e atento ao facto de que o meio investigativo consistente em tecnologia avançada põe o Estado numa posição de forças superior ao arguido, o legislador deverá relacionar a concessão desta intrusão sub-reptícia ao caráter igualmente tecnológico do delito. Do mesmo modo, deve resguardar o núcleo essencial da vida privada, determinando a exclusão sumária de todos os dados que revelem aspetos pertencentes ao setor intangível e não sindicável que possam ser ofensivos para a dignidade humana.

Uma vez implementado o aparato de investigação extrassensorial e decorrido o seu prazo de atuação, a lei deve obrigar a disponibilização de todo o material apreendido, especificando as funcionalidades utilizadas e o código fonte do programa informático espião.

Dada a já anunciada volatilidade da prova digital, o relatório com toda a atividade técnica desenvolvida necessitará de certificar que o sistema objeto da invasão não tenha sido penetrado por instrumento semelhante ao utilizado pela investigação, capaz de forjar provas incriminadoras contra o visado.

No que respeita aos requisitos orgânicos, o investigador considera que apenas o magistrado judicial estará apto a decidir pela concessão de infiltração por meio de *malware*. Isto porque, uma vez que as constituições em Portugal e no Brasil referem que, em casos de ameaça a direitos fundamentais, não poderá ser afastada a apreciação judicial.

No caso específico da República Federativa do Brasil de 1988, defende-se a existência de uma exceção legal aos poderes de investigação oriundos de comissão parlamentar de inquérito. Caso contrário, estará dada a possibilidade de denegação e vulneração dos mencionados direitos fundamentais ocorrer, inclusivamente por razões que viriam a ser de cunho político, e sem o necessário conhecimento técnico e imparcialidade judicial para tomada de decisão.

Por estas mesmas razões, a presente investigação procura defender que a decisão não poderia ser tomada pela Polícia Judiciária ou Ministério Público para posterior ratificação pelo juiz.

[267]A técnica de acionamento remoto do microfone de um dispositivo informático é conhecida como Roving Bug (MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software.* Salvador: Editora JusPodivm. 2020, p. 176 — 184)

CONCLUSÕES

Na medida das restrições existentes no corpo da pesquisa, foi possibilitada a demonstração de aplicações no âmbito de investigações por parte das forças de segurança apresentadas pelos programas informáticos conhecidos como *malware*, as espécies dentro das quais estão classificados (vírus, *worms, logic bombs, trojan horses, rootkits, spyware, bot)*, bem como os modos de instalação clássicos, complementando com o exemplo dos avanços obtidos no que respeita a simplicidade e eficácia neste desígnio, com a chamada instalação do «clique zero».

A descoberta de novos *exploits* existentes nos sistemas informáticos e a programação de código malicioso são uma área na qual o Estado pode ter interesse, nomeadamente através da produção de *malware* para uso próprio, ou da aquisição de tais programas informáticos por meio de compra.

Conforme ficou demonstrado, é possível compreender que este aparato pode ser o único capaz de driblar as proteções que a criptografia estabelece para aceder a sistemas informáticos inteiros ou ficheiros específicos. O mesmo se diga acerca deste modo de autoproteção, quando está presente naquilo que respeita a comunicações de pacotes de dados pela rede mundial de computadores em aplicações que disponibilizam serviços de ligações telefónicas por VoIP, ou mesmo durante a utilização de métodos anonimizadores, como é exemplo o programa TOR.

No que corresponde à história do *malware*, desde o seu surgimento até ao seu emprego como indispensável método oculto de investigação, ressaltou-se traços técnicos e jurídicos daquilo que se passou nos EUA, em Espanha e na Alemanha, eleitas para este efeito por serem as representações razoavelmente mais próximas das realidades técnicas e jurídicas verificadas em Portugal e no Brasil.

Concluímos que os países que serviram de parâmetro têm já uma regulamentação expressa em normas processuais penais, sendo apresentado um déficit específico em relação ao modelo legislativo existente na nação norte-americana. Além disto, foi possível observar uma diversidade de nomenclaturas atribuídas ao meio sub-reptício, além de uma variedade de funcionalidades para as quais são permitidas ativações no contexto de uma fase de investigação pré-processual.

Foi averiguado que nenhuma das nações de língua estrangeira sondadas teria adotado o termo «*malware*» nas respetivas leis, conquanto não se tenha constatado um termo mais

adequado para distingui-lo como método de aquisição oculta de fontes de prova em ambiente digital.

Em face da independência e dissemelhança entre o código arbitrário do Estado e as outras ferramentas que, atualmente, fazem parte do arcabouço em mãos dos órgãos públicos de investigação criminal, defende-se a adoção do vocábulo em lei, especialmente pelo que consta da literatura acerca do tema voltada para a comunidade de língua portuguesa.

O processo penal, na qualidade de instrumento constitucional para a garantia dos direitos fundamentais e limitação do *jus puniendi* do Estado, não pode prescindir da regulamentação em lei clara e minuciosa, para legitimação do deferimento de ordem judicial que possibilite investigação por meio de *malware*.

Tal missão a cargo dos legisladores de Portugal e da República Federativa do Brasil de 1988 deve trazer a lume esta indispensável regulamentação legal, observando os requisitos do catálogo de crimes, a delimitação dos sujeitos submetidos a intervenção, a existência de fortes elementos indicativos do cometimento do crime, as funcionalidades que poderão ser ativadas durante sua utilização, a delimitação dos locais onde tais funcionalidades poderão ser ativadas, designadamente se dentro ou fora do domicílio, a garantia de conhecimento do visado após o fim da medida, a reserva jurisdicional para a concessão da medida, o lapso temporal de prevalência da intervenção, bem como os parâmetros de proporcionalidade e subsidiariedade em sua concessão.

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». *In Madhuri, Vol. 9; Hacking. ICFAI University Press*. Vol.6 (1): 167 – 191. Abril de 2009

ADAMS, Devin M. «The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, "Particularly" Speaking». Obtido de *University of Richmond Law Review*, Vol. 51: http://lawreview.richmond.edu/files/2017/03/Adams-513. pdf. 2017 (consultado pela última vez em 02/05/2021)

ALBRECHT, Hans-Jorg. «Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos». AA.VV. *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.* Coimbra: Coimbra Editora. 2009

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

ALEXY, Robert. «Derechos fundamentales, ponderación y racionalidad». *Revista Iberoamericana de Derecho Procesal Constitucional*, n.º 11. Jan. — jun. de 2009

ALEXY, Robert. *Teoria dos Direitos Fundamentais.* (V. A. Silva, Trad.) São Paulo: Malheiros Editores LTDA. 2008

AMBOS, Kai. «Las prohibiciones de utilización de pruebas en el proceso penal alemán». AA.VV. *Prueba y Proceso Penal — Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado.* Valência: Tirant lo Blanch. 2008

ANDRADE, José Carlos Vieira de. *Os Direitos Fundamentais na Constituição Portuguesa de 1976* (6.ª ed.). Coimbra: Edições Almedina. 2019

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

ANDRADE, Manuel da Costa. «Domicílio, intimidade e constituição: anotação crítica ao Acórdão 364/2006 do Tribunal Constitucional». R*evista Brasileira de Ciências Criminais,* Vol. 100. São Paulo. Jan. – fev. de 2013

ANDRADE, Manuel da Costa. «Métodos Ocultos de Investigação (Plädoyer para uma teoria geral)». AA.VV. *Que futuro para o Direito Processual Penal? Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*. Coimbra: Coimbra Editora. 2009

ANTUNES, Maria João. *Direito Processual Penal* — 2.ª ed. Coimbra: Almedina. 2018 (Versão eletrónica)

AQUILINA, James M; CASEY, Eoghan; MAIL, Cameron H. *Malware Forensics: Investigating and analyzing malicious code.* Burlington: Syngress Publishing. 2008.

ASSOCIATION OF CHIEF POLICE OFFICERS. A*CPO Good Practice Guide For Digital Evidence* — 4.ª ed. 2012, (Disponível em https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_ Practice_Guide_for_Digital_Evidence_v5.pdf; consultado pela última vez em 06/05/2020)

AYCOCK, John. *Computer Viruses and Malware.* EUA: Springer. 2006

BADGER, Lee; GLANCE, Tim; PATT-COMER, Robert; VOAS, Jeff. «Cloud computing synopsis and recommendations». *NIST Special Publication*. Maio de 2012

BATISTA, Lydie Jorge. «O Malware como Meio de Obtenção de Prova em Processo Penal». *Dissertação de Mestrado em Ciências Jurídico-Forenses.* Faculdade de Direito — Universidade de Lisboa. 2018

BICKFORD, Jeffrey et al. «Rootkits on smart phones: Attacks, implications and opportunities». *Proceedings of the 11th International Workshop on Mobile Computing Systems and Applications.* Annapolis: Maryland. 2010

BRASIL. Plenário do Supremo Tribunal Federal. ADcI 5468/DF de 29/06/2016. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5468_voto_MCM.pdf (consultado pela última vez em 15/02/2021)

BRENNER, Susan W. «At the ligth speed: attribution and response to cybercrime/terrorism/warfare». *Jornal of Criminal Law and Technology*, Vol. 97, n.º 2. 2007

BRENNER, Susan W. «Law, Dissonance and Remote Computer Searches». *North Carolina Journal of Law & Technology*, Vol. 14, n.º 1. 2012

BRENNER, Susan W. *Cybercrime — Criminal Threats from Cyberspace.* California: ABS-CLIO, LLC. 2010

BRITO, Beatriz Seabra de. *Novas Tecnologias e Legalidade da Prova em Processo Penal.* Coimbra: Almedina. 2021

BRITZ, Marjie T. *Computer Forensics and Cyber Crime: An Introduction* — 3.ª ed. New Jersey: Prentice Hall. 2013

CAIRES, João Gouveia de. «O registo de som e imagem e as escutas ambientais», em *Direito da Investigação Criminal e da Prova* (coord. Maria Fernanda Palma/Carlota Pizarro de Almeida/Dias, Augusto Silva/Mendes, Paulo de Sousa), Coimbra: Almedina. 2014

CAIRES, João Gouveia de. «O regime processual especial aplicável ao crime organizado (económico-financeiro): âmbito de aplicação da Lei n.º 5/2002, de 11 de Janeiro, o regime do sigilo e do registo de voz e imagem». AA.VV. *Direito Penal Económico e Financeiro.* Coimbra: Coimbra Editora. 2012

CAMPOS, Juliana. *O Malware como Meio de Obtenção da Prova em Processo Penal.* Coimbra: Edições Almedina. 2021 (Versão eletrónica)

CANOTILHO, José Joaquim Gomes. *Direito Constitucional e Teoria da Constituição.* Coimbra: Almedina. 2003

CARRELL, N. «Spying on the mob: United States V. Scarfo — A constitutional analysis.» *University of Illinois Journal of Law, Technology e Policy,* n.º 1. 2002

CASEY, Eoghan. «Foundations of Digital Forensics». AA.VV. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* — 3.ª ed. Academic Press/Elsevier. 2011

CASEY, Eoghan; DAYWALT, Christopher. «Computer Intrusion». *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet* — 3.ª ed. Academic Press/Elsevier, 2011

CASTELLS, Manuel. *A Galáxia Internet — Reflexões sobre internet, negócios e sociedade.* Rio de Janeiro: Zahar. 2003

CLOUGH, Jonathan. *Principles of Cybercrime.* Cambridge: Cambridge University Press. 2010

Concelho da Europa. *Electronic Evidence Guide — A basic guide for police officers, prosecutors and judges — Versão 1.0.*, 2013

CONLAN, Kevin; BAGGILI, Ibrahim; BREITINGE, Frank. «Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy». *Digital Investigation*, Vol. 18. 2016. Disponível em: https://www.sciencedirect.com/science/article/pii/S17422876 16300378; consultado pela última vez em 25/03/2021)

CORREIA, João Conde. «A distinção entre prova proibida por violação dos direitos fundamentais e prova nula numa perspectiva essencialmente jurisprudencial». *Revista do CEJ,* n.º 4. 2006

CORREIA, João Conde. «Questões práticas relativas à utilização de diários íntimos como meio de prova em processo penal». *Revista do CEJ,* n.º 5. 2007

CORREIA, João Conde. «Prova digital: as leis que temos e as leis que deveríamos ter». *Revista do Ministério Público*, n.º 139. Julho — setembro de 2014

CORREIA, Miguel Pupo; SOUSA, Paulo Jorge. *Segurança no Software.* Lisboa: FCA, 2.ª Ed. 2017

GONZÁLES-CUÉLLAR SERRANO, Nicolás. «Garantias constitucionales de la persecución penal en el entorno digital». AA.VV. COLOMER, Juan Luis Gómez. *Prueba y Proceso Penal — Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado*. Valência: Tirant to Blanch. 2008

Decisão do BGH de 21/2/2006 — 3BGs 31/06, disponível em BeckRS 2006, 18459: https://beck-online.beck.de/Dokument?vpath=bibdata%5Cents%5Cbeckrs%5C2006%5Ccont%5Cbeckrs.2006.18459.htm&einzelDokumentenKauf=True (consultado pela última vez em 15/06/2021)

DELGADO MARTÍN, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones.* Madrid: Wolters Kluwer. 2016 (Versão eletrónica)

Despacho BGH de 31/1/2007 – StB 18/06, disponível em BeckRS 2007, 1978: https://beck-online.beck.de/Dokument?vpath=bibdata%5Cents%5Cbeckrs%5C2007%5Ccont%5Cbeckrs.2007.01978.htm&einzelDokumentenKauf=True (consultado pela última vez em 15/06/2021)

DIAS, Jorge de Figueiredo. «O Processo Penal Português: problemas e prospectivas». AA.VV. *Que futuro para o Direito Processual Penal? Simpósio de Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português.* Coimbra: Coimbra Editora. 2009

DUPONT, Benoit. «Hacking the Panopticon: Distributed online surveillance and resistance». *Sociology of Crime, Law and Deviance*, Vol. 10. 2008

Endpoint Surveillance Tools (CIPAV). Obtido de *Electronic Frontier Foundation*: https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav. 2011

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

Europol. *Malware Basics.* Obtido de https://www.europol.europa.eu/sites/default/files/documents/malwarebasicscomplete.pdf

Federal Rules of Criminal Procedure. «Rule 41. Search and Seizure». Obtido de *Legal Information Institute, Cornell Law School*: https://www.law.cornell.edu/rules/frcrmp/rule_41 (consultado pela última vez em 05/02/2021)

FILIOL, Eric. *Computer viruses: from theory to applications.* França: Spienger. 2005

GARCIMANTÍN MONTERO, Regina. *Los médios de investigación tecnológicas en el proceso penal.* Navarra: Editorial Aranzadi. 2018 (Versão eletrónica)

GERCKE, Marco. *Understanding Cybercrime: A Guide for Developing Countries.* Genebra: ITU. 2009

GRAHAM, James et al. *Cyber Security Essentials.* Boca Roton: Taylor and Francis. 2011

GUO, Yinghua; SLAY, Jill. «Data recovery function testing for digital forensic tools». Kam-Pui CHOW; Sujeet SHENOI, *Advances in Information and Communication Technology.* Berlim: Springer. 2010

GUTHEIL, Mirja et al. «Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices: Study for the LIBE Committee». *Policy Department for Citizens' Rights and Constitutional Affairs*. 2017 (consultado pela última vez em 2/6/2021)

HOMSTER, Chet. «Discovery Hidden Evidence». *Journal of Digital Forensics Practice*, Vol. 1, n.º 1. 2006

HORNUNG, Gerrit; SCHNABEL, Christoph. «Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention». *Computer Law & Security review*, Vol. 25, n.º 2. 2009

Judgment of 27 February 2008 — 1 BvR 370/07. Obtido de Bundesverfassungsgericht: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html

KENT, Karen; CHEVALIER, Suzane; GRANCE, Tim; DANG, Hung. «Guide to Integrating Forensic Techniques into Incident Response». *NIST Special Publication 800-86*, Maryland: NIST. 2006

KERR, Orin S. «Searches and seizure in a digital word». *Harvard Law Review*, Vol. 119. 2005

KERR, Orin S. «The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"». *Connecticut Law Review,* Vol. 33, 2001

KOCHHEIM, Dieter. «Onlinedurchsuchung und Quellen-TKÜ in der Strafprozessordnung – Neuordnung der tiefen technischen Eingriffsmaßnahmen in der StPO seit dem 24.8.2017». *KriPoz, Ed. 2*. 2018

LÁZARO DOMÍNGUEZ, F. *Introducción a la Informática Forense.* Madrid: Ra-Ma. 2013

LIMA, Renato Brasileiro de. *Manual de Processo Penal: Volume Único* — 9.ª Ed. rev., ampl. e atual. Salvador: Editora JusPodivm. 2021

LOPES, José Mouraz; CABREIRO, Carlos Antão. «A emergência da prova digital na investigação da criminalidade informática». *Sub judice: Justiça e Sociedade*, n.º 35. Abr. — jun. de 2016

MANSON, Stephen; SENG, Daniel Seng (eds.). *Electronic Evidence* — 4.ª Ed. London: Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London. 2017

MARCACINI, A. T. *Direito e Informática: uma abordagem jurídica sobre a criptografia.* São Paulo: Editora Forense, 2002

MARCZAK, Bill et al. «The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit». *Citizen Lab Research Report, n.º 135*. 2020. [Disponível em: https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/ (acedido pela última vez em 06/06/2021) e https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-pernicious-invisibility-of-zero-click-mobile-attacks/?sh=4ae65d5c3079 (acedido pela última vez em 06/06/2021)]

MARTÍNEZ MARTÍNEZ, Ricard. «En torno a la consideración jurídica del numero IP». *Anuario Multidisciplinar para la modernización de las Administraciones Públicas*, n.º 1. 2005

MASON, Stephen; GEORGE, Esther. «Digital evidence and 'cloud' computing». *Computer Law & Security Review*, Vol. 27. 2011

MENDES, Paulo de Sousa. *Lições de Direito Processual Penal.* Coimbra: Almedina. 2013

MENDES, Carlos Hélder C. Furtado. *Tecnoinvestigação Criminal: Entre a Proteção de Dados e a Infiltração por Software*. Salvador: Editora JusPodivm. 2020

MENKE, Fabiano. «A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão». AA.VV. MENDES, Gilmar F.; SARLET, Ingo W.; COELHO, Alexandre Z. P. *Direito, Inovação e Tecnologia.* São Paulo: Saraiva. 2015 (Versão eletrónica)

MESQUITA, Paulo Dá. «Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português — o Código e a Lei do Cibercrime». Em *Processo Penal, Prova e Sistema Judiciário.* Coimbra: Coimbra Editora. 2010

MOHAY, George; ANDERSON, Alison; COLLIE, Byron; VEL, Oliver de; MCKEMMISH, Rod. *Computer and Intrusion Forensics.* Massachusetts: Artech House, Inc. 2003

MOURA, José Souto de. *A Protecção dos Direitos Fundamentais no Processo Penal.* Coimbra: Almedina. 2005

MUÑOZ CONDE, Francisco. *La búsqueda de la verdad en el proceso penal.* Buenos Aires: Hammurabi. 2000

NOVELINO, Marcelo. *Manual de Direito Constitucional* — 8.ª ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: MÉTODO. 2013

OLIVEIRA, Luís Pedro Martins de. «Da autonomia dos regimes das proibições de prova». AA.VV. *Prova Criminal e direito de Defesa — Estudos sobre a teoria da prova e garantias de defesa em processo penal.* Coimbra: Almedina. 2010

ORTIZ PRADILLO, Juan Carlos. «Desafíos legales de las diligencias de investigación tecnológica». AA.VV. *El Proceso Penal – Cuestiones Fundamentales.* Valência: Tirant to Blanch. 2017

ORTIZ PRADILLO, Juan Carlos. «Fraude y anonimato en la red: cuestiones constitucionales y procesales de la desanonimización de la red TOR». Em C. S. Crespo, *Fraude Electrónico – Su gestión penal y civil.* Valência: Tirant to Blanch. 2015

ORTIZ PRADILLO, Juan Carlos. «Remote Forensic Software as a tool for Investigating Cases of Terrorism». *ENAC*. Outubro de 2009

OWSLEY, Brian L. «Beware of Government Agents Bearing Trojan Horses». *Akron Law Review,* Vol. 48, Tomo 2. 2015

PATIL, Nilesh; LINGAM, Chelpa. «Anonymous connections and onion routing». *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, n.º 2. Fevereiro de 2012

PFEFFERKORN, Riana. *The Risks of "Responsible Encryption".* The Center for Internet and Society. 2018 (Disponível em: http://cyberlaw.stanford.edu /files/publication/files/2018-02-

05%20Technical%20Response%20to%20Rosenstein-Wray%20FINAL.pdf, consultado pela última vez em 25/03/2021)

POULSEN, Kevin. «FBI's PC spy malware tactics revealed». Obtido de https://www.wired.co.uk/ (consultado em 03/05/2021)

PRICE, Donald Justin. «The analog and digital word». J. J. Barbara, *Handbook of Digital and Multimedia Forensic Evidence.* Nova Jérsia: Humana Press. 2008

PROJETO DE LEI DO SENADO n.º 33, de 2013, Artigo 3.º, §2.º, da República Federativa do Brasil (Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/113947; consultado pela última vez em 05/07/2020)

RAMALHO, David Silva. «A investigação criminal na Dark Web». *Revista de Concorrência e Regulação,* Ano IV, n.º 14/15. Abr. — set. de 2013

RAMALHO, David Silva. «A recolha de prova penal em sistemas de computação em nuvem». *Revista de Direito Intelectual*, n.º 2. 2014

RAMALHO, David Silva. «O uso de *malware* como meio de obtenção de prova em processo penal». *Revista de Concorrência e Regulação,* Ano IV, nº 16. Out. — dez. de 2013

RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina. 2017

RAMOS, Vânia Costa. «Introdução aos problemas da obtenção de prova em contexto transacional e à proposta da instituição de uma decisão europeia de investigação». Em *Direito da Investigação Criminal e da Prova.* Coimbra: Almedina. 2014

REAL, Rui Miguel dos Santos. «Apreensão, exame ou perícia e utilização processual de meios de prova existentes em material informático (documentos, correio electrónico, memorandos pessoais, fotografias, registos, áudio, etc). Enquadramento jurídico, prática e gestão processual.» *Meios de obtenção de prova e medidas cautelares e de polícia.* Lisboa: CEJ. 2019

RODRIGUES, Anabela Miranda. *Inteligência Artificial no Direito Penal*. Edições Almedina. 2020 (Versão eletrónica, acessível em: https://ebooks.almedina.net/books/978972408 9676)

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

RODRIGUES, Benjamim Silva. *Da Prova Penal — Tomo IV – Da Prova Electrónico-Digital e da Criminalidade Informático-Digital.* Lisboa: Rei dos Livros. 2011

ROGALL, Klaus. «A nova regulamentação da vigilância das telecomunicações na Alemanha». *2.º Congresso de Investigação Criminal.* Coimbra: Almedina. 2010

ROMERO SANCHEZ, Angelica. «Proceso penal, privacidad y autodeterminación informativa en la persecución penal de la delincuencia organizada. Un análisis desde la perspectiva del derecho procesal penal alemán.» *Revista Criminalidad*, Vol. 57(2). 2015

SALT, Marcos. *Nuevos desafios de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos* — 1.ª ed. Buenos Aires: Ad-hoc. 2017

SEIÇA, Alberto Medina de. «Legalidade da prova e reconhecimentos atípicos em processo penal: notas à margem de jurisprudência 'quase' constante». AA.VV. *Liber discipulorum para Jorge de Figueiredo Dias.* Coimbra: Coimbra Editora. 2003

SHEETZ, Michael. *Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers.* New Jersey: John Wiley & Sons. 2007

SHINDER, Debra Littlejonh. *Scene of the Cybercrime: Computer Forensics Handbook.* Massachusetts: Syngress. 2002

SILVA, Flávio Manuel Carneiro da. «Apreensão e utilização processual de meios de prova existentes em material informático». Em *Meios de obtenção de prova e medidas cautelares e de polícia.* Lisboa: CEJ. 2019

SILVA, Germano Marques da. *Curso de Processo Penal II.* Lisboa: Verbo. 2011

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo* — 32.ª ed. rev. e atual. São Paulo: Malheiros. 2009

SILVA, Ricardo Sidi Machado da. *A Interceptação das Comunicações Telemáticas no Processo Penal*. Dissertação de Mestrado em Direito Processual. Faculdade de Direito – Universidade de São Paulo. 2014

SINROD, Eric J.; REILLY, William P. «Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws». *Santa Clara Computer and High Technology Law Journal,* Vol. 16, n.º 2. 2000

ŠKORVÁNEK, Ivan; KOOPS, Bert-Jaap; NEWELL, Bryce Clayton; ROBERT, Andrew. «"My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking» (Pre-Press Draft). *BYU Law Review*, 10. Fevereiro de 2019

SOINÉ, Michael. «Die strafprozessuale Online-Durchsuchung». *NStZ,* n.º 9. 2018 (consultado pela última vez em 15/06/2021)

SOLOVE, Daniel J. *Conceptualizing Privacy*. Califórnia: California Law Review. 2002

TEIXEIRA, Tarcisio et al. «Criptografia e segurança de redes: considerações gerais e a sua inserção no WhatsApp». *Belo Horizonte: Revista da Faculdade de Direito da Universidade Federal de Minas Gerais,* n.º 71. Julho — dezembro de 2017

THOMPSON II, Richard M. *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure.* Obtido de Congressional Research Service: https://fas.org/sgp/crs/misc/R44547.pdf. Setembro de 2016

U.S. Government Info. CIVIL ACTION NO. 4:13-CV-3291 Disponível em: https:// www.govinfo.gov/content/pkg/USCOURTS-txsd-4_13-mj-00234/pdf/USCOURTS-tx sd-4_13-mj-00234-0.pdf ; consultada pela última vez em 06/06/2021.

VACCA, John R. *Computer and Information Security Handbook.* Massachusetts: Elsevier. 2012

VACIAGO, Giuseppe e RAMALHO, David Silva. «Online searches and online surveillance – the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings». *Digital Evidence and Electronic Signature Law Review*. 2016

WEBER, Rolph e HEINRICH, Ulrike I. *Anonymization.* Londres: Springer. 2012

WINTER, Lorena Bachmaier. «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015». *Boletín del Ministerio de Justicia,* Ano LXXI, n.º 2195. 2017 Obtido de: https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/InstLibraryDoctrinalStudies/1701_Estudio.pdf (consultado pela última vez em 10/07/2021)

WOO, Christopher; SO, Miranda. «The Case for Magic Lantern: September 11 Highlights — The need for Increased Surveillance». *Harvard Journal of Law & Technology*, Vol. 15, n.º 2. 2002

ZARAGOZA TEJADA, Javier Ignacio. «El registro remoto de equipos informáticos». Em *Investigación Tecnológica y Derechos Fundamentales: Comentarios a las modificaciones introducidas por la Ley 13/2015*. Navarra: Editorial Aranzadi. 2017 (Versão eletrónica)

ÍNDICE

INTRODUÇÃO 10

1. O *MALWARE* 12

1.1. Definição do problema 12

1.2. Conceito e classificação 13

1.3. Métodos viáveis para a instalação 21

2. O RECURSO AO *MALWARE* NO DIREITO COMPARADO 24

2.1. A admissibilidade do *malware* nos Estados Unidos da América (EUA) 24

2.2. A admissibilidade do *malware* em Espanha 32

2.3. A admissibilidade do *malware* na Alemanha 35

3. A LIMITAÇÃO DA ATIVIDADE PROBATÓRIA EM PROCESSO PENAL IMPOSTA PELOS DIREITOS FUNDAMENTAIS 43

3.1. A legalidade como condição procedimental em investigação criminal 43

3.2. A restrição de direitos fundamentais durante o uso de *malware* como ferramenta de investigação estatal 48

4. TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO, PRESSUPOSTOS PARA RECOLHA DA PROVA DIGITAL E AS MEDIDAS ANTIFORENSES 56

4.1. Tecnologias da Informação e Comunicação (TIC) 56

4.2. Pressupostos para a recolha da prova digital: a cadeia de custódia 57

4.3. Medidas antiforenses: a criptografia, o projeto TOR e a esteganografia 64

5. REQUISITOS PARA CONSTRUÇÃO DE UM REGIME JURÍDICO QUE POSSIBILITE O USO DA TÉCNICA DE *MALWARE* EM INVESTIGAÇÕES CRIMINAIS 72

5.1. A inadmissibilidade do uso da técnica de *malware* em investigações criminais em Portugal 72

5.2. A inadmissibilidade do uso da técnica de *malware* em investigações criminais no Brasil 77

5.3. Requisitos materiais, formais e orgânicos 80

CONCLUSÕES 83

BIBLIOGRAFIA 85