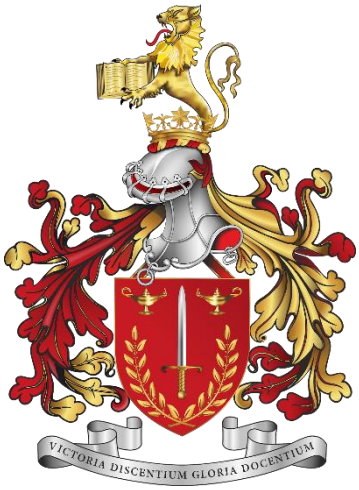

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

DO FUNDAMENTO, ÂMBITO E LIMITES DA PESQUISA DE DADOS INFORMÁTICOS ENQUANTO MEIO DE OBTENÇÃO DE PROVA

Hernâni Carvalho Correia Pinto

Dissertação de Mestrado em Ciências Policiais

Área de Especialização em Criminologia e Investigação Criminal

Orientação científica:

Professor Doutor José Fontes

Lisboa, dezembro de 2020.

“– Vais começar a aproximar-te do paraíso, Fernão, no momento em que atingires a velocidade perfeita. E isso não é voar a mil e quinhentos quilómetros por hora, nem a um milhão, nem à velocidade da luz. É que nenhum número é um limite e a perfeição não tem limites.”

Fernão Capelo Gaivota, de Richard Bach

AGRADECIMENTOS

À minha mulher, Carla Correia Pinto, e aos meus filhos Dinis e João, pela paciência e palavras de encorajamento constantes, que se revelaram absolutamente determinantes na concretização do presente trabalho.

Aos meus pais, Francisco e Antónia, e irmão, André, pelo apoio permanente. Sei que posso contar sempre com eles.

Ao Senhor Professor Doutor José Fontes, que gentilmente aceitou orientar a presente dissertação, pelo seu acompanhamento, disponibilidade e conselhos valiosos.

Ao meu amigo e companheiro nesta caminhada, José Garcia, pela paciência, palavras de incentivo e espírito de entreajuda.

À minha amiga Maria Irene Magalhães, pela sua generosidade e disponibilidade.

Às minhas queridas amigas Cláudia Correia e Inês Leite e ao amigo e colega Nuno Cabral, pela prontidão com que aceitaram ajudar a rever esta dissertação.

Ao ISCPSI e, em especial, a todos os docentes do XI Curso de Mestrado em Ciências Policiais - Área de Especialização em Criminologia e Investigação Criminal, por impulsionarem os conhecimentos na área das Ciências Policiais, tornando-o um centro académico de referência e de cultivo de valores humanos que em muito enriquecem os alunos.

Uma palavra também de apreço, pelas iniciativas levadas a cabo no 2.º ano do curso de Mestrado, destacando o seminário de "Elaboração da dissertação" e o do 4.º Colóquio, dirigidos pelo Senhor Professor Luís Guerra, que, num ano especialmente difícil, ainda assim, permitiram o debate, esclarecimento de dúvidas, e a obtenção de sugestões pertinentes.

Aos colegas do Curso de Mestrado, pela partilha de conhecimentos e debates profícuos.

Por último, não menos importante, a todos os que fazem parte da Unidade Nacional de Combate ao Cibercrime, pela sabedoria e generosidade com que transmitem os conhecimentos no âmbito da investigação do cibercrime e pelos

estímulos ao constante processo de aprendizagem, o que foi determinante na escolha deste tema. Um bem-haja a todos!

“As leis do cibercrime (…) são más e são insuficientes, estando na hora de ser alteradas”. A experiência e o conhecimento adquiridos já permitem superar as suas deficiências e criar um sistema que, sem esquecer o nível ideal de proteção dos direitos fundamentais, contribua para a eficácia da justiça penal. Assim haja vontade e imaginação legislativa” (Conde Correia, 2014).

RESUMO

Os avanços tecnológicos dos últimos anos trouxeram inegáveis benefícios para a economia e para a sociedade. No entanto, também foram aproveitados pelos criminosos, designadamente para gizar novos *modi operandi* relativamente aos crimes tradicionais e para desenvolver uma panóplia de novas práticas criminosas, tornando-se o fenómeno do cibercrime uma realidade cada vez mais preocupante e com tendência crescente.

A consciência desta nova realidade e a necessidade de criar respostas adequadas à repressão do cibercrime estiveram na origem da Convenção sobre o Cibercrime do Conselho da Europa, aberta à assinatura em Budapeste em 23 de novembro de 2001.

Portugal veio a adaptar o direito interno à Convenção sobre Cibercrime do Conselho da Europa, através da Lei 109/2009, de 15 de setembro, também designada por Lei do Cibercrime. Esta lei consagra novos meios de obtenção de prova em ambiente digital, destacando-se a pesquisa de dados informáticos, prevista no art.º 15.º da Lei do Cibercrime.

Não obstante se tratar de um meio de obtenção de prova com bastante relevância para a investigação criminal, a vulgarização de soluções tecnológicas, tais como a encriptação, poderão inviabilizar a recolha de prova digital, que ficará dependente da colaboração do visado.

Simultaneamente aperfeiçoam-se novos meios tecnológicos com um potencial inegável para a efetivação da recolha de prova digital, mas com a particularidade de se tratarem de meios ocultos ao visado. É o caso do *malware*.

Assim sendo, tendo presente estas circunstâncias, e a necessidade de consagrar meios eficazes no combate a uma criminalidade cada vez mais sofisticada, urge proceder à alteração da lei do cibercrime, prevendo-se de forma clara e detalhada a pesquisa de dados informáticos de forma remota e sem o conhecimento do visado, através de meios informáticos adequados, em consonância com os princípios e valores jurídico-constitucionais.

Através destes princípios, será possível encontrar critérios axiológicos capazes de delimitar o correto âmbito de aplicação e os limites à aplicabilidade deste meio de obtenção de prova.

PALAVRAS-CHAVE

Prova digital; meios de obtenção de prova em ambiente digital; pesquisa de dados informáticos; encriptação; *malware*, princípios constitucionais.

ABSTRACT

The latest years' technological breakthroughs have brought undeniable benefits to both economy and society. Nevertheless, they were also seized by perpetrators, namely to find new *modi operandi* for their usual criminalities and to develop new criminal practices, hence becoming the cybercrime phenomenon. This is a growing tendency as well as an ever-distressing reality.

The awareness of this new reality and the need to create suitable answers to limit cybercrime were at the origin of the Council of Europe Cybercrime Convention, open for signature in 23 November 2001, in Budapest.

Portugal adapted its national law to the Council of Europe Cybercrime Convention through the law 109/2009 of 15 September, also named as cybercrime law. This law dedicates new means of obtaining electronic evidence, standing out the electronic data research, which is in art.15º of the Cybercrime law.

Although electronic data research is a relevant means of evidence for securing the criminal investigation, the widespread use of IT solutions, as for example, encryption may render the electronic evidence useless and reliant on the good will of the perpetrator.

At the same time, new IT solutions are getting streamlined with undisputable potential for helping on the effective acquisition of the electronic evidence plus having the distinctiveness of being concealed to the perpetrator. This is the case of malware.

Thus, mindful of these circumstances and of the necessity to dedicate effective means to fight the increasingly sophisticated criminality, it is of utmost urgency to change the cybercrime law in a clear and detailed way. The objective would be to provide for remote research of electronic data without the suspect's knowledge, through the appropriate IT tools in accordance with the constitutional law's principles and values.

By means of these principles, it will be possible to find axis criteria capable of outlining the right scope of implementation and the boundaries of the enforcement of this type of evidence acquisition.

KEYWORDS

Digital evidence; means of electronic evidence acquisition; search data; encryption; *malware*, constitutional law principles.

SIGLAS, ACRÓNIMOS E ABREVIATURAS

Ac. — Acórdão

al. — alínea

APA — *American Psychological Association*

ARPANET — *Advanced Research Projects Agency Network*

art.º — artigo

CART — *Computer Analysis Response Team*

CEHD — Convenção Europeia dos Direitos do Homem

CIPAV — *Computer and Protocol Address Verifier*

CP — Código Penal

CPP — Código de Processo Penal

CRP — Constituição da República Portuguesa

DL — Decreto-Lei

ECTEG — *European Cybercrime Training and Education Group*

EXIF — *Exchangeable Image File Format*

FBI — *Federal Bureau of Investigation*

HTML — *Hypertext Markup Language*

IMEI — *International Mobile Equipment Identity*

IOCE — *International Organization on Computer Evidence*

IOCTA — *Internet Organised Crime Threat Assessment*

IoT — *Internet of Things*

IP — *Internet Protocol*

JIC — Juiz de Instrução Criminal

MAC — *Media Access Control*

MD5 — *Message-Digest Algorithm*

MP — Ministério Público

NASA — *National Aeronautics and Space Administration*

NIST — *National Institute of Standards and Technology*

NIT — *Network Investigative Technique*

OPC — Órgão de Polícia Criminal

PDF — *Portable Document Format*

PGP — *Pretty Good Privacy*

P2P — *Peer-to-peer*

RAM — *Random Access Memory*

RCS — *Rich Communication Services*

SHA-1 — *Secure Hash Algorithm*

SOCTA — *Serious Organised Crime Threat Assessment*

SMS — *Short Message Service*

SWGDE — *Scientific Working Group on Digital Evidence*

TOR — *The Onion Router*

TEDH — Tribunal Europeu dos Direitos do Homem

TRE — Tribunal da Relação de Évora

TRL — Tribunal da Relação de Lisboa

TRP — Tribunal da Relação do Porto

UFED — *Universal Forensic Extraction Device*

MODO DE CITAR

As citações e as referências bibliográficas serão efetuadas de acordo com a norma APA (6.ª edição).

ÍNDICE

INTRODUÇÃO

I. CONSIDERAÇÕES INTRODUTÓRIAS

Nas últimas décadas registou-se um crescimento vertiginoso associado às tecnologias de informação e de computação.

Tais avanços tecnológicos permitiram uma evolução sem precedentes, com inegáveis benefícios para a economia e sociedade, ao ponto de se caracterizar a presente época como a "Era da Internet e o prenúncio do fim da geografia" (Ramalho, 2017, p. 46), "aldeia global" (McLuhan, citado em Poiares, 2019) ou realidade à distância de um *click* (Ramos, 2014).

Foi há pouco mais de cinquenta anos que se viu surgir computadores, que ocupavam salas inteiras e eram utilizados apenas por instituições específicas da sociedade norte-americana, designadamente a NASA e algumas Universidades (Ramos, 2014).

Posteriormente, em 1969, surge uma rede que ligava computadores geograficamente distantes, cuja designação era ARPANET (*Advanced Research Projects Agency Network*) e que tinha uma forte ligação ao Departamento de Defesa dos Estados Unidos da América, visto que visava a troca de informação pelos militares de forma segura. Em 1983 a ARPANET passa a designar-se por internet (Antunes & Rodrigues, 2018).

Em 1973, a Motorola apresentou o primeiro telemóvel: o DynaTAC[1].

Passados cinquenta anos os computadores e dispositivos eletrónicos suscetíveis de ligação à internet fazem parte da nossa vida diária. Com efeito, evidencia-se que, atualmente, existem mais de quatro mil milhões de utilizadores de internet, verificando-se ainda que 40% da população mundial está conectada à internet[2].

O aumento do volume de dados gerados pelos utilizadores na internet foi de tal forma exponencial que potenciou a computação na *cloud* permitindo o

[1] https://observador.pt/2017/04/04/foi-ha-44-anos-que-apareceu-o-primeiro-telemovel/ (acedido a 24/11/2019).

[2] *Vide www.internetlivestats.com* (consultado no dia 24/11/2019).

armazenamento desses mesmos dados em servidores, cuja localização física muitas vezes se desconhece.

Prevê-se que a rede 5G represente mais um passo de gigante para a tecnologia, possibilitando a criação de condições ideais para impulsionar a internet das coisas (IoT).

No entanto, estes avanços tecnológicos também foram aproveitados para gizar novos *modi operandi* relativamente aos crimes tradicionais, apontando-se como exemplo o tráfico de droga, que vem recorrendo a mercados *online* na *darknet* ou a prática de burlas com recurso à internet. Fala-se, a este, respeito da "deslocalização criminosa para a *Web*" (Venâncio, 2011, p. 15).

Paralelamente emergiram novos tipos de ilícitos criminais, tais como a falsidade informática, sabotagem informática, acesso ilegítimo, entre outros (Nunes D. R., 2018).

Em 2008, foram apontados cinco fatores potenciadores desta nova realidade: o primeiro prende-se com a redução de custo dos bens tecnológicos; o segundo com a redução do custo do acesso à internet; o terceiro está relacionado com a expansão rápida da banda larga; o quarto enfatiza "o aumento do conhecimento e o acesso por parte de possíveis ofensores a técnicas e métodos de ocultação de provas digitais, nomeadamente, técnicas de encriptação, compressão digital, a esteganografia, entre outros"; o último refere o acréscimo da literacia computacional por parte da comunidade global de internautas" (Santos, Bessa, & Pimentel, 2008, pp. 6-7).

Nos dias de hoje, constata-se o aumento crescente de utilizadores de internet que utilizam diversas formas de se anonimizar, a expansão dos mercados digitais *online, na dark web,* de venda de produtos ilícitos, inacessíveis através dos comuns *browsers,* a utilização cada vez mais frequente da moeda virtual, cuja utilização permite ocultar a identidade do seu proprietário, a vulgarização de aplicações de comunicação que utilizam criptografia ponto-a-ponto, sem ser necessária qualquer configuração adicional, bem como a vulgarização de programas informáticos de encriptação que garantem a proteção do conteúdo dos diversos dispositivos informáticos.

Esta realidade encontra-se amplamente evidenciada, nomeadamente nos relatórios da Europol: SOCTA (*Serious and Organized Crime Threat Assessment*) de 2017 e IOCTA (*Internet Organized Crime Threat Assessment*) de 2019[3].

A consciência das mudanças provocadas pela digitalização e pela globalização permanente das redes informáticas e o objetivo de proteger a sociedade contra a criminalidade no ciberespaço vieram a originar a Convenção sobre o Cibercrime do Conselho da Europa, aberta à assinatura em Budapeste em 23 de novembro de 2001. Portugal assinou, nessa mesma data, a Convenção, que entrou em vigor na ordem jurídica internacional a 1 de julho de 2004.

No entanto foi só através da Lei 109/2009, de 15 de setembro, também designada por Lei do Cibercrime que se viria a transpor para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação e a adaptar o direito interno à Convenção sobre Cibercrime do Conselho da Europa**.**

Conforme se alcança, logo no art.º 1.º da Lei do Cibercrime, *a presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico*.

Assim, nos artigos 12.º a 19.º encontram-se previstos os meios de obtenção de prova que, na esteira do previsto na Convenção sobre Cibercrime do Conselho da Europa, visam dotar as autoridades competentes dos necessários poderes de investigação e de combate a esta nova área da criminalidade. Evidencia-se ainda que, de acordo com o disposto no art.º 11.º, e tendo presente as respetivas exceções, o âmbito de aplicação destas disposições processuais não se circunscreve aos crimes previstos nesta lei, podendo ser utilizados, nomeadamente, quando seja necessário proceder à recolha de prova em suporte eletrónico (Nunes D. R., 2018).

[3] O relatório SOCTA está disponível em https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment e o IOCTA em https://www.europol.europa.eu/iocta-report.

Atendendo à inexistência, no ordenamento jurídico nacional, de qualquer definição de prova digital, a doutrina tem vindo a propor soluções, que permitem preencher esse vazio legal. Assim sendo, Benjamim Silva Rodrigues refere que a "prova digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digital de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital" (Rodrigues, 2011, p. 39). Por sua vez, Armando Dias Ramos refere que se trata de "toda a informação passível de ser obtida ou extraída de um dispositivo digital (local, virtual ou remoto) ou de uma rede de comunicações" (Ramos, 2014, p. 86).

Deste modo, relativamente aos meios de obtenção de prova digital consagrados na Lei do Cibercrime, que irão ser objeto de análise ao longo da presente dissertação, o art.º 12.º reporta-se à preservação expedita de dados; o art.º 13.º à revelação expedita de dados de tráfego; o art.º 14.º à injunção para apresentação ou concessão do acesso a dados; o art.º 15.º à pesquisa de dados informáticos; o art.º 16.º à apreensão de dados informáticos; o art.º 17.º à apreensão de correio eletrónico e registos de comunicações de natureza semelhante; o art.º 18.º à interceção de comunicações e o art.º 19.º às ações encobertas.

Não obstante as medidas adotadas pelos Estados no combate ao cibercrime, elucida Elias (2018) que:

> Uma combinação de fatores de ordem legal e técnica, negam aos órgãos de polícia criminal, o acesso, de forma atempada, às comunicações eletrónicas suspeitas e a possibilidade de execução de perícias forenses. Em muitos casos, as dificuldades colocadas pelos sistemas de encriptação e de retenção de dados, reduzem a possibilidade de prossecução das investigações e recolha de prova digital de forma célere, eficaz e eficiente (p. 341).

Face a estes obstáculos, afigura-se essencial que os métodos de obtenção de prova em processo penal "acompanhem o caminho do progresso,

contando que o potencial de lesividade e de devassa do mundo científico e digital sejam harmonizados com os valores jurídico-constitucionais essenciais de um Estado de Direito democrático" (Brito, 2018, p. 25).

Neste contexto, destaca-se o papel da Ciência Forense Digital que se tem desenvolvido, num esforço assinalável e fundamental de dotar as polícias de investigação criminal de meios para fazer face a esta nova realidade.

Os contributos da Ciência Forense Digital têm vindo a ser determinantes no âmbito de investigações criminais em que seja necessário recolher prova em sistemas informáticos[4], possibilitando ainda a adaptação dos meios de obtenção de prova à evolução técnico-científica que se encontra em permanente mudança.

II. PROBLEMA DE INVESTIGAÇÃO E JUSTIFICAÇÃO DO TEMA

No âmbito destes meios de obtenção de prova, surge o problema de investigação subjacente à dissertação que se pretende desenvolver e que consiste em analisar a pesquisa de dados informáticos, prevista no art.º 15.º da Lei do Cibercrime, de modo a perceber o seu fundamento, o âmbito de aplicação e os limites deste meio de obtenção de prova e se o mesmo, atendendo ao tempo entretanto decorrido, desde que foi previsto legalmente e ao avanço tecnológico que entretanto também se verificou, se afigura como adequado para a investigação criminal.

O presente trabalho de investigação parte do interesse do autor, que desempenha funções de investigação criminal. No âmbito dessas funções, a temática da recolha de prova digital, tem-se colocado com bastante acuidade, quer no que diz respeito ao enquadramento legal, quer às dificuldades relacionadas com a sua obtenção. Trata-se, portanto, de um trabalho "inspirado por uma angústia pessoal na qual se enxerta a experiência profissional" (…)

[4] O conceito de sistema informático consta do art. 2.º al. a) da Lei do Cibercrime, tratando-se de *qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção.*

esperando-se que este “subjetivismo inevitável deixe no problema uma marca singular que, longe de se opor à ciência, a enriquece com as perspetivas originais de cada um” (Deshaies, 1992, pp. 52, 180), não se olvidando que, no âmbito do trabalho de investigação, “o interesse do investigador é assumir uma atitude científica, distanciada e neutra” (Coutinho, 2014, p. 21).

Este trabalho de investigação insere-se no campo epistemológico do Direito Processual Penal, não se perdendo de vista as relações de “interpenetração que medeiam entre a Constituição e o processo penal, traduzidas na conhecida síntese de Henkel: o Direito Processual Penal como verdadeiro Direito Constitucional aplicado” (Costa Andrade, 2013, p. 12). Atendendo ao facto deste meio de obtenção de prova poder aproveitar os avanços da Ciência Forense Digital, também se recorrerá aos conhecimentos que a mesma tem produzido neste âmbito, nos últimos anos.

Face ao exposto, entende-se ainda, salvo melhor opinião, que o objeto de estudo que se propõe realizar será pertinente para as Ciências Policiais. Na verdade, conforme ensina Elias “as Ciências Policiais procuram dotar a organização policial e os polícias de conhecimento, de capacidades e competências adequadas (…) a ciência e a técnica estreitam laços, procurando o aprofundamento do conhecimento e o aperfeiçoamento da práxis.” (2018, p. 48). É também este contributo que se pretende oferecer.

Com efeito, “é através da investigação que se reflete e problematizam os problemas nascidos na prática, que se suscita o debate e se edificam as ideias inovadoras.” (Coutinho, 2014, p. 6).

Efetuada uma revisão de literatura, com vista a determinar o estado da arte acerca desta temática, constata-se que, nos últimos anos, tem havido um interesse crescente pela área do cibercrime e da ciberinvestigação, que se traduziu na realização de diversos estudos, designadamente sobre os meios de obtenção de prova previstos na Lei do Cibercrime. Por razões metodológicas, a estes se fará referência, oportunamente, no âmbito das temáticas que vierem a ser abordadas.

O presente estudo pretende efetuar uma análise numa perspetiva de maior enfoque no âmbito e limites deste específico meio de obtenção de prova,

que é a pesquisa de dados informáticos, considerando a evolução tecnológica, entretanto operada, que poderá representar novas oportunidades para as polícias de investigação criminal, mas também se poderá traduzir num obstáculo à obtenção de elementos de prova digital. É o que sucede com a encriptação.

A este respeito afigura-se útil a analogia com o cumprimento de um mandado de busca, quer seja domiciliária ou não, no âmbito do qual poderá haver necessidade de recorrer ao arrombamento. Como proceder no caso de uma "busca digital", ou seja de uma pesquisa de dados informáticos, em que um determinado sistema se encontra protegido com encriptação e o seu proprietário não revela as credenciais de acesso? O que se se poderá equiparar, em termos tecnológicos, a um arrombamento. Poder-se-á recorrer, por exemplo, a programas forenses, também designados pela doutrina como *malware*[5] sem o conhecimento do visado, para aceder ao conteúdo de um sistema informático?

Este tipo de programas forenses têm vindo a ser consagrados em diversos ordenamentos jurídicos. No nosso ordenamento jurídico tem-se vindo a discutir, designadamente, o seu enquadramento na ação encoberta. Porém, é sabido que esta solução tecnológica poderá comportar várias funcionalidades, que poderão ir da mera aquisição de elementos, suscetíveis de servir de prova num dado sistema informático e num momento determinado, à interceção de dados em tempo real ou, em última instância à ativação do teclado, da câmara ou do microfone de um determinado dispositivo informático.

No que tange aos limites da pesquisa de dados informáticos, cuidar-se-á de analisar o recurso aos programas forenses, sem o conhecimento do visado, como forma de dar sentido útil a este particular e importante meio de obtenção de prova, num cenário de dispositivo encriptado em que o visado não revela as credenciais de acesso ao mesmo.

Pelo exposto anteriormente, com a elaboração da presente investigação, pretende-se abordar a pesquisa de dados informáticos, enquanto meio de

[5] Segundo explica Silva Ramalho, de forma detalhada, o termo *malware* resulta da contração do adjetivo *malicious* (malicioso) e do substantivo *software* (programa informático), sendo que no contexto de investigação criminal, poderá ser utilizado, designadamente para monitorizar a atividade do suspeito ou apropriação de dados informáticos suscetíveis se servir de prova (Ramalho, 2017, pp. 318-319).

obtenção de prova, previsto no art.º 15.º da Lei do Cibercrime, procurando perceber numa tripla vertente, a sua *ratio legis*, o seu âmbito de aplicação e os seus limites, face às normas constitucionais, tendo presente que a utilização dos dispositivos eletrónicos e da internet se assume com grande importância na concretização e enquanto meio facilitador da prática de crimes.

Para alcançar estes objetivos ir-se-á estruturar a presente dissertação em quatro capítulos.

No primeiro capítulo, procurar-se-á traçar a evolução legislativa em Portugal, no que tange à recolha de prova digital e enunciar os meios de obtenção de prova consagradas na Lei do Cibercrime. Importará ainda recortar o âmbito de aplicação destes institutos jurídicos face ao regime da pesquisa de dados informáticos e apreensão dos mesmos.

O segundo capítulo visará identificar os principais contributos da Ciência Forense Digital. Este ramo da ciência tem evoluído de forma significativa e apresentado soluções que se afiguram bastante relevantes na recolha de prova digital e apresentação da mesma em tribunal.

O terceiro capítulo consistirá na apresentação sumária de soluções entretanto consagradas nos ordenamentos jurídicos da Alemanha, Espanha e França, tendo-se escolhido estes países, desde logo por razões de proximidade geográfica com o nosso ordenamento jurídico e pelo facto de se saber que estes permitem a realização da pesquisa de dados informáticos de forma remota e sem o conhecimento do visado.

No quarto capítulo procurar-se-á traçar os limites da pesquisa de dados informáticos face aos valores e princípios constitucionais consagrados no nosso ordenamento jurídico.

Por último, antes de se concluir o presente estudo, procurar-se-á, *de iure condendo,* apresentar contributos para uma proposta de regime jurídico que possa ser mais adequado à realização da justiça sempre sem olvidar o respeito pelos direitos fundamentais dos cidadãos.

III. MÉTODO

O presente estudo foi iniciado com a premissa de que “uma investigação é, por definição, algo que se procura. (Quivy & Campenhoudt, 2005, p. 31). Para alcançar este propósito é necessário empregar meios adequados que representem “uma economia de esforços tendo em vista alcançar o fim esperado.” (Deshaies, 1992, p. 27).

Por sua vez, Larenz (1997) ensina, na sua obra *Metodologia Da Ciência do Direito,* que a necessidade e a justificação de um método decorre do significado, da especificidade estrutural do seu objeto de estudo.

Sendo certo que a palavra método tem origem no termo grego *methodus,* cujo significado é precisamente seguir um caminho com vista a atingir um determinado fim (Poças, 2020, p. 17), então a questão que desde logo se impõe é a de qual o método a adotar para realizar uma investigação jurídica.

Esta questão torna-se ainda mais premente pela escassez de literatura no que tange à metodologia da investigação em Direito.

Sendo o Direito uma ciência pragmática, sempre com vista a prosseguir a justiça, que visa resolver problemas suscitados pela vida real, consubstanciada na conhecida expressão *quid iuris,* então “a matéria-prima do investigador são as normas jurídicas” (Poças, 2020, pp. 21,26).

Com efeito, para o Direito não se poderá chegar a uma solução inconclusiva, a um *non liquet.* O problema suscitado tem que ser resolvido, sendo certo que a problematização se coloca com especial enfoque no âmbito das respostas que venham a ser encontradas, dado que as mesmas precisam de ser sustentadas com argumentos que possam ser aceites pela comunidade científica, antecipando-se potenciais críticas (*Idem*).

Ora para levar a cabo esta tarefa de compreensão do sentido das normas jurídicas, com vista à sua aplicação a um determinado caso concreto da vida real, assume especial relevância a análise doutrinal interpretativa destas normas, afigurando-se ainda relevante a análise dedutiva, a analogia e a análise política (Chynoweth & Gomes, 2010).

Sendo certo que muitas normas jurídicas poderão ser ambíguas ou pouco claras, será ainda relevante para a sua interpretação perceber o contexto

histórico e social das mesmas ou compreender, de forma adequada, a realidade que a norma pretende disciplinar, ou seja, a sua teleologia (*Idem*).

Este labor não pode olvidar que a tarefa de desvendar o sentido da norma, cerne da hermenêutica jurídica, no âmbito da temática dos meios de obtenção de prova em processo penal, implica compreender o papel fundamental e de quadro normativo de referência da Constituição que consagra valores e princípios fundamentais (Cunha, 2018).

Deste modo, a investigação irá incidir na análise bibliográfica de doutrina relacionada com o tema apresentado e jurisprudência, que em muito contribuem para densificar o sentido das normas jurídicas, bem como das soluções consagradas noutros ordenamentos jurídicos, pese embora as normas jurídicas assentem num determinado contexto histórico e social.

Salienta-se ainda que o objeto da presente dissertação está relacionado com a informática forense, o que poderá tornar mais complexo o desenvolvimento do tema. Assim sendo, tendo presente que a interdisciplinaridade poderá enriquecer a abordagem jurídica, tentar-se-á abordar as principais questões que se podem suscitar com interesse para o cumprimento dos objetivos enunciados, afigurando-se ainda necessário o recurso às obras e artigos científicos que permitam alcançar esse desiderato.

1. DA CONVENÇÃO DE BUDAPESTE À LEI DO CIBERCRIME

No âmbito deste capítulo analisar-se-á a evolução legislativa em matéria de prova digital.

Recuando no tempo, já em 11/09/1995, no âmbito da Recomendação n.º R (95) 13, do Conselho da Europa, se fazia notar a falta de meios adequados para obter prova digital e, consequentemente desenvolver investigações criminais[6].

No entanto, é consensual afirmar-se que o marco fundamental no combate ao cibercrime e na recolha de prova digital é a Convenção do Conselho da Europa Sobre Cibercrime, ETS n.º 185, também conhecida por Convenção de Budapeste. Este tratado de Direito Internacional foi elaborado entre 1997 e 2001 (Verdelho, 2004, p.125), tendo contado com a participação de peritos internacionais de todo o mundo (Venâncio, 2011, p. 23).

Com efeito, na génese da Convenção estava a consciência da rápida evolução da tecnologia e da sua utilização para fins criminosos que se tornou num problema de difícil resolução, tendo em conta as lacunas no quadro legal existente em matéria de cooperação judiciária e policial.

Nesta sequência, o Comité Europeu para os Problemas Criminais procedeu à criação, em novembro de 1996, através da Decisão CDPC/103/211196, de um Comité de Peritos sobre a Cibercriminalidade no Ciberespaço, tendo o mesmo sido mandatado para proceder à elaboração de um instrumento jurídico eficaz. Este Comité veio a concluir os trabalhos em finais do ano 2000, que estiveram na base do primeiro esboço da Convenção sobre a Cibercriminalidade (Rodrigues, 2011).

A 22 de junho de 2001, o Comité Europeu para os assuntos criminais veio a aprovar o projeto de Convenção sobre a Cibercriminalidade.

[6] Este documento pode ser acedido em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 (Consultado a 05/01/2020).

No dia 19 de setembro de 2001, os Delegados dos Ministros do Conselho da Europa aprovaram o texto da Convenção, que veio a ser adotado em 8 de novembro de 2001 pelo Comité dos Ministros (Rodrigues, 2011, p. 330).

Tendo sido aberta à assinatura a 23 de novembro de 2001, Portugal foi um dos trinta países que assinou, nessa mesma data, a Convenção, que entrou em vigor na ordem jurídica internacional a 1 de julho de 2004[7] [8].

Conforme refere Pedro Verdelho, este instrumento de direito internacional tem "vocação universal, pretendendo vir a ser aceite pela generalidade das jurisdições do globo. E bem se percebe porquê. Nas redes informáticas, na Internet, as fronteiras políticas e geográficas deixaram de fazer sentido" (Verdelho, 2004, p. 125).

Esta Convenção assenta assim em três eixos: a modernização e harmonização das legislações no que concerne ao direito substantivo, a eficácia do processo penal, no que concerne às novas infrações, mas também relativamente a ilícitos criminais que utilizam sistemas informáticos e em que seja necessário recolher prova digital e, por último, a cooperação internacional[9].

A estrutura da Convenção reflete a importância destes eixos, repartindo-se em quatro capítulos: o primeiro capítulo diz respeito à terminologia; o capítulo segundo, às medidas a tomar a nível nacional, englobando as temáticas do Direito Material e do Direito Processual; o capítulo terceiro enfoca na Cooperação Internacional e o capítulo quarto estabelece as cláusulas finais.

Apesar de Portugal ter sido um dos primeiros países a assinar a Convenção de Budapeste, a mesma só veio ser aprovada pela Assembleia da República, através da Resolução n.º 88/2009 e pelo Decreto do Presidente da República n.º 92/2009, ambos publicados a 15 de setembro de 2009 (Venâncio, 2011).

---

[7] *Vide* a Convenção sobre o Cibercrime em: http://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0 (Consultado a 05/01/2020).

[8] Mais informação relativamente aos países que assinaram e ratificaram a Convenção poderá ser consultada em: https://www.coe.int/en/web/conventions/recent-changes-for-treaties/ (acedido a 05/01/2020).

[9] A este respeito cumpre salientar o ponto 16 do Relatório Explicativo da Convenção Sobre o Cibercrime que poderá ser acedido em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (Consultado a 05/01/2020).

Neste seguimento, através da Lei 109/2009 – Lei do Cibercrime, publicada na mesma data, Portugal viria a transpor para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação e a adaptar o direito interno à Convenção sobre Cibercrime do Conselho da Europa**.**

Esta lei veio substituir a Lei da Criminalidade Informática – Lei n.º 109/91, de 17 de agosto[10].

Salienta-se que o quadro normativo de 1991 teve origem na Recomendação R (89) 9 do Conselho da Europa e visava definir e punir práticas criminosas que se designou por crimes informáticos (Verdelho, 2009).

A Lei do Cibercrime não se limitou a rever as normas de direito substantivo, aglutinando ainda normas processuais específicas.

Este aspeto merece um especial destaque, tendo em atenção que o ordenamento jurídico português não dispunha de meios adequados e eficazes para a investigação criminal em ambiente digital.

Não é despiciendo referir que já em 2003 tinha estado em discussão, na Assembleia da República, um projeto de lei promovido pelo grupo parlamentar do partido popular – projeto de lei n.º 217/IX, de 27 de janeiro de 2003, que visava a criação de um Regime Jurídico da Obtenção de Prova Digital Eletrónica na internet (Venâncio, 2006). Todavia, essa iniciativa viria a caducar, por força da dissolução da Assembleia da República.

Em 2004, seria o Governo a elaborar uma proposta legislativa sobre a mesma matéria. No entanto, esse projeto não chegaria ao Conselho de Ministros (Santos, Bessa, & Pimentel, 2008).

Se é compreensível a criação de um diploma próprio para a cibercriminalidade, conforme resulta dos argumentos aduzidos na Exposição de Motivos da Proposta de Lei n.º 289/X/4ª[11]: "a geral inconveniência de ver em

[10] Esta Lei pode ser consultada em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=151&tabela=lei_velhas&nversao=1&so_miolo= (Acedida a 16/02/2020).

[11] A Exposição de Motivos da Proposta de Lei n.º 289/X/4ª está acessível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d76574339305a58683062334d76634842734d6a67354c5667755a47396a&fich=ppl289-X.doc&Inline=true (consultada em 16/02/2020).

diplomas estruturantes do ordenamento penal regras especiais" e "a conveniência prática, para os operadores judiciários, de ver sistematizados todos os normativos referentes a um setor específico da criminalidade", o mesmo não se pode dizer relativamente às normas processuais.

Com efeito, conforme se alcança do art.º 11.º n.º 1, alíneas b) e c), da Lei do Cibercrime, estas normas aplicam-se quer aos crimes cometidos por meio de um sistema informático[12], quer em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, consagrando-se assim um regime geral em matéria de recolha de prova digital, suscetível de ser aproveitado na investigação de qualquer crime[13].

Neste seguimento, sufraga-se a posição defendida por Paulo Dá Mesquita, segundo a qual se impunha a integração das regras processuais constantes do capítulo III da Lei do Cibercrime, no Código de Processo Penal, fazendo todo o sentido um novo capítulo intitulado "Da prova eletrónica" no âmbito do título III do CPP ("Dos meios de Obtenção de Prova") (Dá Mesquita, 2010, p. 101).

1.1. A ESTRUTURA DA LEI DO CIBERCRIME

A Lei do Cibercrime, conforme resulta do seu art.º 1.º, *estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico (…) adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa*.

A estrutura desta lei reparte-se, à semelhança do que sucede na Convenção sobre o Cibercrime, em cinco capítulos. No capítulo I encontra-se a referência ao objeto da lei e definições. O capítulo II trata das disposições penais materiais. O Capítulo III regula as disposições processuais, que serão objeto de

[12] Acerca da definição de "sistema informático" *vide* nota de rodapé 4.
[13] Neste sentido, *Vide* Duarte Nunes (Nunes D. R., 2018, p. 18), Paulo Dá Mesquita (Dá Mesquita, 2010, p. 98) e Pedro Dias Venâncio (Venâncio, 2011, p. 91).

análise adiante. O capítulo IV diz respeito à cooperação internacional. Por último, o capítulo V estabelece as disposições finais e transitórias.

Descrita a estrutura da Lei do Cibercrime, cumpre evidenciar, que as medidas previstas nos artigos 12.º a 17.º representam "um conjunto integrado de medidas processuais que devem ser analisadas e aplicadas como um todo, pois em muitos aspetos práticos se relacionam e complementam" (Venâncio, 2011, p. 99).

Com efeito, a *ratio* destas normas é, essencialmente, o acesso aos dados informáticos[14] tendo em vista as finalidades específicas de uma determinada investigação criminal.

Sendo certo que o escopo da presente dissertação é a análise da pesquisa de dados informáticos, recortando o seu âmbito de aplicação face aos restantes meios de obtenção de prova previstos na Lei do Cibercrime, importa previamente abordar, ainda que de forma sintética conceitos essenciais que possibilitem uma melhor compreensão dessas normas legais.

1.2. O ENDEREÇO IP E A INVESTIGAÇÃO CRIMINAL

Um desses conceitos que importa desde logo abordar é o de endereço IP (*Internet Protocol*).

A internet, enquanto "infraestrutura de interligação de redes de computadores (…) disponibiliza serviços que são implementados por servidores que aceitam os pedidos realizados por clientes" (Antunes & Rodrigues, 2018, pp. 4,7).

O leque de serviços disponibilizados pela internet é muito vasto e engloba serviços de correio eletrónico, *sites web,* redes sociais, motores de busca, entre outros.

Deste modo, quando um computador ou outro dispositivo, tal como um *smartphone* se liga à internet, identifica-se nessa rede em dois níveis: lógico,

[14] O conceito de dados informáticos consta do art.º 2.º, al. b) da Lei do Cibercrime, tratando-se de "qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função.

através do endereço IP e físico, também conhecido como endereço de *hardware* ou MAC (*Media Access Control*), visto que através deste se identifica fisicamente a placa de rede do computador (Antunes & Rodrigues, 2018).

O endereço IP trata-se assim de um "protocolo de comunicação de pacotes de dados utilizado para encaminhar e transportar informação na internet ou em outras redes" (Santos, Bessa, & Pimentel, 2008, p. 233) e assume grande relevância para a investigação criminal pois, à partida, poderá identificar a localização dos equipamentos na rede internet, além de delimitar a área em que os mesmos estão localizados (*Ibidem*).

Através de fontes abertas[15] na internet, é possível consultar diversas informações acerca dos endereços IP que poderão estar relacionados com a prática de ilícitos criminais, de entre essas informações evidencia-se a identificação do Fornecedor de Serviços de Internet[16].

O Fornecedor de Serviços de Internet poderá assim, quando questionado relativamente à utilização de um determinado endereço IP, identificar o respetivo cliente. Esta informação será relevante, designadamente, para ponderar, em termos de estratégia de investigação criminal, a realização de uma pesquisa de dados informáticos com vista à recolha de eventuais elementos probatórios.

Atendendo ao aumento exponencial de utilizadores de internet, o endereçamento IPv4, vigente desde 1982, limitado a 4.294.967.296 de endereços, revelou-se incapaz de atribuir um IP fixo a todos os sistemas informáticos (Cybercrime Division, 2014, p. 96).

Como forma de ultrapassar esta limitação, os Fornecedores de Serviços passaram a atribuir endereços dinâmicos.

Assim, quando um cliente desliga a sua ligação à internet, o mesmo endereço IP poderá ser utilizado por outro cliente que entretanto se tenha ligado, podendo-lhe também ser atribuído, durante sua utilização, mais do que um endereço IP.

---

[15] Fontes abertas de informação são fontes acessíveis por terceiros. Contrapõem-se às fontes fechadas de informação que implicam um pedido formal das autoridades (Antunes & Rodrigues, 2018, pp. 193-195).

[16] Exemplo destes repositórios de informação são os *sites*: http://centralops.net/co/ e whois.domaintools.com (Consultados a 29/02/2020).

Deste modo, para se chegar ao utilizador deste endereço importa precisar, no pedido dirigido ao Fornecedor de Serviços, a data/hora da comunicação que efetivamente se pretende (*Ibidem*).

O endereçamento IPv6, não obstante ter surgido em 1991 (Santos, Bessa, & Pimentel, 2008) e apresentar a vantagem de atribuir um endereço IP estático a cada sistema informático[17], ainda não se encontra generalizado.

1.3. ACERCA DA PROVA DIGITAL

Outro conceito fundamental e prévio no âmbito desta temática é o de prova digital, salientando-se que a compreensão do conceito de prova digital e das suas características encontra-se estreitamente relacionado com os meios de obtenção de prova que se irão analisar.

Segundo a definição constante do *Eletronic Evidence Guide*, publicado pelo Conselho da Europa, a prova digital é qualquer tipo de informação que tenha sido criada, armazenada ou transmitida por meio digital que venha a ser necessária para provar ou refutar um determinado facto no âmbito de um processo judicial (Cybercrime Division, 2014, p. 11).

Já houve ensejo de referir a ausência, na legislação portuguesa, de qualquer definição de prova digital. Tal facto, conforme referido por Silva Ramalho, "acabou por criar espaço para que a jurisprudência e a doutrina preenchessem o vazio" (Ramalho, 2017, p. 99).

Assim, Benjamim Silva Rodrigues refere que a "prova digital pode definir-se como qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digital de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital" (Rodrigues, 2011, p. 39).

Por sua vez, Armando Dias Ramos refere que se trata de "toda a informação passível de ser obtida ou extraída de um dispositivo digital (local, virtual ou remoto) ou de uma rede de comunicações" (Ramos, 2014, p. 86).

[17]O IPv6 permitirá um número máximo de endereços IP únicos de 340.282.366.920.938.463.463.374.607.431.768.211.456 (Ramalho, 2017, p. 53).

No que concerne às características da prova digital, importa identificar as mesmas, de modo a perceber os condicionalismos inerentes à sua obtenção. Assim sendo, tomar-se-á por base os ensinamentos de Benjamim Silva Rodrigues (Rodrigues, 2011, pp. 42-43).

A primeira característica apontada por este autor é efemeridade, salientando-se assim a necessidade de celeridade na sua recolha.

A prova digital é também frágil e volátil. Estas características exigem uma abordagem específica e adequada por parte de quem executa a recolha de prova digital. Com efeito, uma manipulação descuidada poderá implicar a alteração das suas propriedades ou até a sua eliminação. A este respeito, Silva Ramalho apresenta como exemplos a alteração de um ficheiro que é editado e que ocorre após a sua gravação, ou a possibilidade de um terceiro aceder remotamente à prova a fim de proceder à sua alteração ou até mesmo eliminação (Ramalho, 2017).

Outra característica que também exige uma abordagem técnica e conhecimentos científicos adequados é a complexidade ou codificação, isto porque o acesso a sistemas informáticos implica desde logo conhecer as respetivas palavras-passe. Refira-se também a aparente imaterialidade ou não visibilidade, isto porque nem sempre é possível identificar com facilidade o elemento probatório que se pretende. É o caso dos metadados dos ficheiros, a que voltará mais adiante.

Por último, importa referir a dispersão da prova digital, que implica que a mesma poderá ser localizada geograficamente em diferentes locais, pelo que será necessário solicitá-la a vários fornecedores de serviços. Esta característica também está relacionada com o facto da prova digital também poder estar alojada em diversos suportes, tais como *pendrives, smartphones* e *tablets*.

Estas características da prova digital implicam para a investigação criminal uma abordagem efetivamente específica e especializada, obviamente distinta dos vulgarmente designados “crimes de cenários”.

Constitui um exemplo ilustrativo e atual o apresentado por Orin Kerr, para perceber as diferenças dos crimes denominados de cenário e os crimes em

ambiente digital ou que seja necessário recolher prova nesse meio (Kerr, 2005, pp. 281-289).

Imaginemos então um indivíduo que concretiza um roubo a um banco, utilizando para tal uma arma de fogo. A abordagem em termos de investigação criminal passará necessariamente por ouvir testemunhas, com vista a identificar o autor ou obter informações relevantes, eventualmente perceber como é que é fisicamente o suspeito, como é que estava vestido, que tipo de arma foi utilizada pelo mesmo para concretizar o assalto, como é que este abandonou o local após ter cometido o crime.

Afigura-se ainda fundamental a inspeção judiciária ao cenário de crime, com vista a recolher eventuais vestígios que o autor possa ter deixado.

Estes vestígios, do ponto de vista sistemático, podem tratar-se de vestígios físicos: orgânicos ou biológicos (cabelos, sangue, saliva), inorgânicos ou não biológicos (fragmentos, tintas, vidros, documentos) e morfológicos (impressões digitais, marcas de objetos, vestígios balísticos) ou vestígios psíquicos ou imateriais, quando se revelam por comportamentos (Braz, 2009, p. 25).

Na sequência das diligências de investigação realizadas e partindo do pressuposto que é identificado um suspeito, poderá ainda ser necessário recorrer aos meios de obtenção de prova, previstos legalmente, tais como revistas, buscas e apreensões de modo a carrear elementos suscetíveis de servir de prova para o processo.

Prosseguindo com o exemplo de Orin Kerr imaginemos agora a versão digital do crime apresentado: um indivíduo que realiza um acesso ilegítimo a um banco, com recurso a um computador e uma ligação à internet, com vista a subtrair dinheiro de uma determinada conta bancária.

Neste caso, o autor “entra” virtualmente na instituição bancária através de uma ligação à internet garantida, num primeiro momento, pelo seu Fornecedor de Serviços de Internet. De forma a ocultar o seu rasto, o autor ligar-se-á a servidores e a Fornecedores de Serviços intermediários, antes de concretizar a subtração de valores.

Sendo certo que no caso apresentado não haverá testemunhas, nem vestígios físicos, a abordagem do investigador criminal terá que ser necessariamente diferente.

Assim, importará desde logo obter junto da instituição bancária visada o registo do endereço IP que acedeu à referida conta bancária e procedeu à movimentação ilícita dos valores. Este elemento permitirá iniciar a reconstituição dos passos do autor, através dos servidores intermediários e ligação à internet efetivamente utilizada, de modo a chegar-se ao endereço IP inicial.

Através deste elemento, será possível obter a identificação de um titular de um contrato de serviços de internet e um endereço de faturação junto do Fornecedor de Serviços de internet. Seguidamente, só realizando uma pesquisa de dados informáticos aos equipamentos aí existentes será possível obter novos elementos para a investigação, evidenciando-se que as características da prova digital já explanadas exigem uma abordagem científica aos sistemas informáticos, de modo a acautelar a correta obtenção da prova digital.

O exemplo de Orin Kerr demonstra, como bem evidencia Silva Ramalho (2017) que:

> A prova digital não pode ser considerada como uma derivação da prova física. Como realidades distintas, que são, deverão ser objeto de diferentes enquadramentos jurídicos, livres das amarras da analogia e da constante fuga para a subsidiariedade de regimes concebidos para a prova física" (p. 104).

Após estas breves referências, estar-se-á em condições de prosseguir com a análise dos meios de obtenção de prova previstos nos artigos 12.º a 17.º da Lei do Cibercrime.

1.4. OS MEIOS DE OBTENÇÃO DE PROVA

1.4.1. A PRESERVAÇÃO EXPEDITA DE DADOS

O primeiro meio de obtenção de prova que se irá analisar encontra-se previsto no artigo 12.º, cuja epígrafe é a preservação expedita de dados.

Esta norma tem origem no artigo 16.º da Convenção sobre o Cibercrime – Conservação expedita de dados informáticos armazenados.

Conforme se alcança do ponto 155 do Relatório Explicativo da Convenção sobre o Cibercrime[18] a preservação de dados é um importante instrumento na investigação do crime informático e, de forma transversal, em crimes cometidos pela internet. Já anteriormente se aludiu à volatilidade dos dados informáticos, o que poderá implicar a sua alteração ou eliminação. Este meio permite dirigir ao administrador desses dados, tratando-se de um destinatário "confiável" (Nunes D. R., 2018, p. 37), uma ordem de preservação, de modo a assegurar de forma célere a integridade dos mesmos.

Assim sendo, nos termos do art.º 12.º n.º 1, a preservação de dados, trata-se de uma ordem dirigida *a quem tenha disponibilidade ou controlo desses dados* visando acautelar que os dados se mantenham "a salvo de toda e qualquer modificação, danificação ou eliminação, a fim de não comprometer a produção de prova, tendo em vista a descoberta da verdade material" (*Idem*, p. 34).

A doutrina e a jurisprudência apresentam uma distinção tripartida entre dados de base, dados de tráfego e dados de conteúdo que importa desde já abordar.

Assim, os dados de base são os dados relativos à conexão à rede, ou seja os elementos fornecidos pelo cliente ao prestador de serviços, designadamente nome e morada, bem como os elementos necessários atribuídos pelo prestador de serviços ao cliente, tais como o número de telefone e "IP estático" (Nunes D. A., 2019, p. 556).

Os dados de tráfego são os "dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e dados gerados pela utilização da rede" (Neves, 2011, p. 210). Estes dados "permitem identificar as comunicações entre o emissor e o destinatário, a data, a hora, a duração da comunicação, a localização de ambos, a frequência das ligações efetuadas" (Nunes D. A., 2019, p. 557).

[18] Acerca deste relatório veja-se a nota de rodapé n.º 9.

Por último, os dados de conteúdo são essencialmente as informações transmitidas por um emissor a um recetor, sendo estes apenas acessíveis através das escutas telefónicas ou interceção de comunicações.

Como se depreende da norma prevista no art.º 12.º da Lei do Cibercrime, esta abrange todo o tipo de dados informáticos armazenados, designadamente dados de tráfego, sendo que a ordem de preservação é emitida pela autoridade judiciária competente. Ora, conjugando a norma do art.º 12.º n.º 2 com o disposto no art.º 1.º, al. b) do CPP, que procede à definição de autoridade judiciária, conclui-se que a competência para emitir a ordem de preservação é do magistrado do MP na fase de inquérito, do JIC na fase de instrução e do Juiz na fase de julgamento.

Porém, o art.º 12.º também prevê que a ordem de preservação seja emitida pelo OPC em duas situações. A primeira, mediante autorização da autoridade judiciária competente, prevendo-se neste caso a possibilidade de delegação de competências por parte da autoridade judiciária (cfr. art.º 270.º e 290.º do CPP). A segunda situação tem fundamento na "urgência ou perigo na demora" (art.º 12.º n.º 2). Com efeito a finalidade desta medida cautelar e de polícia é "obstar a situações de *periculum in mora* em que a obtenção da autorização prévia da autoridade judiciária possa pôr em risco o sucesso da medida, máxime a perda de provas relevantes para a investigação" (Nunes D. R., 2018, p. 49).

Assumindo a natureza de uma medida cautelar e de polícia, o OPC deverá informar de imediato a autoridade judiciária, através da elaboração e envio do relatório previsto no art.º 253.º do CPP (*Vide* art.º 12.º, n.º 2, *in fine*).

Da correlação do art.º 12.º com o art.º 11.º, conclui-se ainda que este meio de obtenção de prova poderá ser utilizado na investigação de qualquer crime (Dá Mesquita, 2010, p. 98)[19].

Relativamente ao teor da ordem de preservação, estabelece o art.º 12.º, n.º 3 que a mesma *discrimina, sob pena de nulidade: a) a natureza dos dados; b) a sua origem e destino, se forem conhecidos;* e *c) o período de tempo pelo qual deverão ser preservados*.

[19] Neste sentido também Duarte Rodrigues Nunes (Nunes D. R., 2018, p. 41).

No que concerne ao período de preservação, estabelece a norma que os dados podem ser preservados por um período máximo de três meses, sendo este período renovável por períodos também não superiores a três meses, desde que se verifiquem os respetivos requisitos de admissibilidade até ao limite de um ano (art.º 12.º n.º 5).

Deste modo, quem tiver a disponibilidade ou o controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, conservando a sua integridade pelo tempo que tiver sido fixado, de modo a permitir às autoridades competentes a sua obtenção, evidenciando-se que a entidade que preserva os dados fica ainda obrigada ao dever de confidencialidade (art.º 12.º n.º 4).

Salienta-se ainda que o regime da ordem de preservação expedita de dados não se pode confundir com o regime estatuído na Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, 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.

Esta lei assume como objeto, nos termos do art.º 1.º, n.º 1, a regulação da conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes.

O elenco de crimes graves consta do art.º 2.º, n.º 1, al. g)[20] deste diploma legal.

Com efeito, sendo certo que a Lei n.º 32/2008, de 17 de julho estabelece no art.º 6.º que os fornecedores de serviços de comunicações eletrónicas devem conservar os dados previstos no art.º 4.º dessa lei pelo período de um ano a contar da data da conclusão da comunicação, nada obsta a que seja emitida uma

[20] "Crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação da moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima."

ordem de preservação ao abrigo do art.º 12.º da Lei do Cibercrime, no último dia do prazo, previsto no art.º 6.º da Lei n.º 32/2008, sendo o prazo da preservação contado a partir desta data nos termos da Lei do Cibercrime. No limite, o prestador de serviços poderá ter que manter estes dados por dois anos, conforme se alcança da interpretação de ambos os preceitos legais a que se aludiu anteriormente (Dias Ramos, 2013, p. 10)[21].

Inexistindo uma consequência expressa para o incumprimento da ordem de preservação, será conveniente a autoridade judiciária cominar como sanção a prática de um crime de desobediência, nos termos do art.º 348.º, n.º 1, al. g) (Nunes D. R., 2018, p. 35)[22].

1.4.2. A REVELAÇÃO EXPEDITA DE DADOS

Na sequência do que vem sendo exposto, tendo por base o art.º 17.º da Convenção sobre o Cibercrime, o art.º 13.º da Lei 109/2009 trata da revelação expedita de dados de tráfego.

Sobre esta norma importa referir que se encontra numa relação de dependência e de garante de eficácia face à preservação expedita de dados (Nunes D. R., 2018), ao estabelecer o dever do fornecedor de serviços a quem foi ordenada a preservação de dados, nos termos do art.º 12.º, ter que indicar, logo que saiba, outros fornecedores de serviços através dos quais uma determinada comunicação tenha sido efetuada.

1.4.3. A INJUNÇÃO

Prosseguindo a análise do elenco de meios de obtenção de prova previstos na Lei do Cibercrime, que apresentam uma relação mais estreita com o objeto do presente estudo, ir-se-á agora abordar a injunção para apresentação

[21] Esta também é a posição adotada por Duarte Rodrigues Nunes (Nunes D. R., 2018, p. 50).
[22] Dias Ramos entende que o incumprimento da ordem de preservação origina de *per si* a prática do crime de desobediência (Dias Ramos, 2013, p. 9).

ou concessão do acesso a dados, prevista no art.º 14.º deste diploma legal e que teve origem no art.º 18.º da Convenção sobre o Cibercrime.

Assim, sendo necessário à produção de prova, tendo em vista a descoberta da verdade material, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente, MP ou Juiz, consoante a fase do processo, pode ordenar a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de incorrer na prática de um crime de desobediência (cfr. art.º 14.º, n.º 1).

Trata-se de um importante meio de obtenção de prova para a investigação criminal, salientando-se assim a possibilidade de obter dados, designadamente junto de Fornecedores de Serviços não cooperantes, que de outra forma seriam de difícil obtenção, atendendo à complexidade inerente à identificação e recolha de informação relevante em ambiente digital (Verdelho, 2004).

No que tange ao objeto desta norma, verifica-se que a ordem dirigida aos fornecedores de serviço poderá abranger a comunicação ao processo dos dados relativos aos seus clientes ou assinantes, *neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, que permita determinar o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço, bem como a identidade, a morada postal ou geográfica e o número de telefone do assinante, qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento disponíveis com base num contrato ou acordo de serviços; ou qualquer outra informação sobre a localização do equipamento de comunicação disponível com base num contrato ou acordo de serviços* (*Vide* art.º 14.º, n.º 4).

Deste modo, ficam abrangidos pela injunção os dados de base ou de localização armazenados, sendo que relativamente a estes últimos, destacam-se “os dados de localização dos sistemas informáticos (incluindo telemóveis, *smartphones*, computadores, etc.), bem como outros dados de localização por GPS, que eventualmente estejam na posse de fornecedores de serviço (Nunes

D. R., 2018, p. 62). Acerca dos dados de tráfego, conforme se referiu, não se poderá olvidar o regime previsto na Lei n.º 32/2008.

Relativamente ao endereço IP, coloca-se a questão de saber se se deve diferenciar o IP dinâmico do IP estático.

Ora segundo a posição vertida na Nota Prática n.º 1/2012 do Gabinete do Cibercrime "o n.º 4, al. b) do art. 14.º regula expressamente o procedimento de solicitação do endereço IP aos operadores de comunicações. Trata-se de um regime especial e independente da categorização de dados definidos na lei"[23]. Com efeito, quando a lei faz referência ao *número de acesso,* pretende efetivamente referir-se ao endereço IP.

Assim sendo,

> é indiferente que se trate de um endereço IP fixo, atribuído a título permanente a um só utilizador, ou de um endereço dinâmico, sucessivamente atribuído a múltiplos utilizadores: ambos são o tal *número de acesso* e em nenhum dos casos a entidade que conduz a investigação fica na posse de dados suscetíveis de revelar informação do foro pessoal ou íntimo.

Com efeito, conforme salienta Conde Correia, "os endereços IP (…) não revelam um concreto utilizador (…) são apenas um conjunto alargado de números, que, isoladamente, nada pode transmitir sobre o seu utilizador individual" (Conde Correia, 2014, p. 49).

Deste modo, segundo a conclusão vertida na referida nota prática:

> A injunção é a forma processual apropriada para que o Ministério Público solicite aos fornecedores de serviços a identificação do endereço IP utilizado por um determinado indivíduo e, na vertente oposta, a identificação do cliente

[23] A Nota Prática n.º 1/2012 do Gabinete do Cibercrime está acessível através de: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_1_pedido_de_ip.pdf (consultada a 05/04/2020).

que usou um determinado endereço IP em determinadas circunstâncias de tempo"[24].

David Silva Ramalho refere ainda que se encontra abrangida, pelo âmbito da norma, a chave de acesso à encriptação dos dados. Deste modo, quando os dados sejam cifrados por uma entidade terceira e se encontrem na sua disponibilidade, a chave poderá ser obtida através de uma injunção (Ramalho, 2017).

Sendo certo que a capacidade de armazenamento dos sistemas informáticos modernos é cada vez maior, o que dificulta a obtenção dos conteúdos que se encontrem guardados nos mesmos, este instrumento legal permite a sua obtenção "compulsivamente, mesmo que tais conteúdos estejam ocultos no sistema, encriptados ou protegidos por *passwords*" (Verdelho, 2015, p. 262).

Salienta-se que este meio de obtenção de prova não pode ser dirigida a arguido ou a suspeito, salvaguardando-se assim o princípio da não auto-incriminação (Neves, 2011), tema este a que se voltará posteriormente. Cumpre realçar, no entanto, que esta norma permite ainda assim interpelar um terceiro a disponibilizar dados relativos quer ao arguido, quer ao suspeito, sob pena de se esvaziar de conteúdo este instrumento legal (Nunes D. R., 2018).

No que diz respeito às limitações legais deste meio de obtenção de prova, salienta-se o disposto no n.º 6 do art. 14.º que estabelece, *prima facie,* a impossibilidade de recorrer à injunção *quanto a sistemas informáticos utilizados para o exercício da advocacia, das atividades médica e bancária e da profissão de jornalista*, sendo o escopo desta norma, de forma clara, a proteção das atividades sujeitas ao dever de sigilo profissional.

[24] Neste sentido, o Ac. do TRL de 19/06/2014. Acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/eb1460fa14510bf380257d080036a9b9?OpenDocument (Consultado a 05/04/2020). Em sentido contra: Duarte Rodrigues Nunes, segundo o qual tratando-se o IP dinâmico de um dado de tráfego, a norma constante do art. 14.º só se aplicará quando as autoridades conhecerem o IP utilizado e esteja apenas em causa saber quem o utilizou num determinado momento. Fora destas situações aplicar-se-á o disposto no art. 18.º da Lei do Cibercrime.

Todavia, no n.º 7 do art.º 14.º estabelece-se que *o regime de segredo profissional ou de funcionário ou de segredo de estado previsto no art.º 182.º do CPP é aplicável com as necessárias adaptações*.

Deste modo, a autoridade judiciária pode ordenar a quebra do sigilo profissional, em situações excecionais, segundo o princípio da prevalência do interesse preponderante, nos termos do disposto no art.º 135 do CPP, *ex vi* art.º 182.º, n.º 2 do CPP.

1.4.4. A PESQUISA DE DADOS INFORMÁTICOS

A norma que prevê a pesquisa de dados informáticos está consagrada no art.º 15.º da Lei do Cibercrime.

A palavra pesquisa, segundo o Dicionário da Porto Editora[25], tem origem no termo latino *perquisa* (procurada cuidadosamente), fazendo-se ainda alusão ao particípio passado de *perquirere* (procurar cuidadosamente).

Esta norma tem origem no art.º 19.º da Convenção sobre o Cibercrime do Conselho da Europa que estabelece desde logo no seu número um que

> *cada parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para proceder a buscas ou aceder de modo semelhante: a) a um sistema informático ou parte do mesmo, bem como a dados informáticos que nele se encontrem armazenados; e b) a um suporte que permita armazenar dados informáticos.*

Da leitura deste artigo e da análise do Relatório Explicativo da Convenção do Cibercrime[26], evidencia-se a este respeito o ponto 191. Segundo este documento, a utilização do termo tradicional busca "traduz a ideia de exercício do poder coercivo por parte do estado e indica que o poder mencionado (nesse artigo) é análogo à busca clássica". O referido documento refere ainda que busca significa "procurar, ler, inspecionar ou rever dados".

---

[25] Acedido em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/pesquisa (consulta a 14/04/2020).

[26] Acerca deste documento *vide* nota de rodapé n.º 9.

Este importante meio de obtenção de prova encontra assim o seu fundamento "na modernização e harmonização das legislações nacionais relativamente à busca e apreensão de dados informatizados armazenados", no âmbito da investigação criminal, como se salienta no ponto 184 do mencionado Relatório Explicativo.

Com efeito, também na Exposição de Motivos da Proposta de Lei n.º 289/X/4ª se refere que a *essência destas medidas processuais, coincide, no âmbito do ciberespaço, com as clássicas formas de busca e apreensão, do processo penal*.

Também Pedro Verdelho refere que a lei adotou a expressão *pesquisa de dados informáticos* "para aquilo que poderia designar-se também como busca informática" (Verdelho, 2009, p. 740).

O n.º 6 do art. 15.º estabelece que à pesquisa de dados informáticos, *são aplicáveis, com as necessárias adaptações as regras de execução de buscas previstas no CPP*.

Entrando agora na análise do art.º 15.º da Lei do Cibercrime, realça-se mais uma vez a possibilidade deste meio de obtenção de prova poder ser utilizado não só no que tange às investigações de crimes cometidos por meio de sistemas informáticos, mas também em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (cfr. art.º 11.º, n.º 1, al. c.).

Da leitura do art.º 15.º n.º 1 resulta que o mesmo poderá ser utilizado quando no "*decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático"*. Deste modo, a pesquisa de dados informáticos poderá incidir, designadamente, sobre os computadores, *tablets, smartphones* e suportes de armazenamento de dados (DVD, CD, cartões de memória, *pendrives*) (Nunes D. R., 2018).

Sendo certo que não se trata de um meio de obtenção de prova de *ultima ratio,* dado que apenas se exige que a diligência se afigure necessária à descoberta da verdade material, configurando assim um meio habitual de recolha de prova digital, a verdade é que se o fim visado pela diligência de investigação puder ser alcançado com outro meio menos gravoso,

designadamente uma injunção para apresentação de dados, então neste caso, deverá ser vedada aos órgãos de polícia criminal a possibilidade de realizar a pesquisa de dados (*Idem*).

No que concerne à competência para autorizar ou ordenar este meio de obtenção de prova, a norma refere que a mesma é da autoridade judiciária competente, sendo que, como já houve ensejo de referir, aquando da análise do regime da preservação expedita de dados, a competência é do magistrado do MP na fase de inquérito, do JIC na fase de instrução e do Juiz na fase de julgamento.

A este respeito, importa mencionar o entendimento de Benjamim Silva Rodrigues, segundo o qual a norma constante do art.º 15.º deve ser interpretada de forma restritiva, obviando-se a possibilidade da autoridade judiciária que ordenou ou autorizou a diligência não presida à mesma, bem como no sentido de que a autorização para a realização desta diligência de investigação criminal tenha de ser judicial, nos termos do art.º 32.º n.º 4 da CRP (Rodrigues, 2010).

Com efeito, "o computador surge-nos cada vez com maior insistência e persistência, como o domicílio informático ou a casa digital onde mora a nossa alma digital" (*Idem*, p. 473). O mesmo se pode dizer do *smartphone,* que segundo publicitado pelos meios de comunicação social, desde 2008 passou a ser o meio preferido de acesso à internet, nomeadamente pelos portugueses[27].

Relativamente à interpretação restritiva defendida por Benjamim Silva Rodrigues, salvo o devido respeito, não se pode acompanhar o entendimento, segundo o qual se torna obrigatória a presença da autoridade judiciária aquando da realização da diligência. Primeiro, porque este entendimento não tem correspondência na letra da lei, que refere de forma perentória que a autoridade judiciária deve presidir à diligência, sempre que possível. Além do mais, essa obrigatoriedade também não se encontra prevista no regime das buscas domiciliárias, cuja essência, como já se referiu, coincide com o regime da pesquisa de dados informáticos.

[27] *Vide*: https://jornaleconomico.sapo.pt/noticias/adeus-pc-ola-telemovel-portugueses-dao-primazia-ao-smartphone-para-aceder-a-internet-358990 (Acedido a 14/04/2020).

Por outro lado, pela mesma lógica de argumentos, à semelhança do que também sucede no regime das buscas domiciliárias, que tem o seu supedâneo legal no art.º 177.º n.º 1 do CPP, parece que a solução mais consentânea com as normas constitucionais, atendendo ao potencial de lesão que este meio implica para os direitos dos cidadãos, deveria ser no sentido da autorização para a pesquisa de dados informáticos ter de ser judicial, esbatendo-se assim a diferença legal, salvo melhor opinião injustificada, entre os regimes legais destes meios de obtenção de prova.

Na verdade, a pesquisa de dados informáticos restringe diversos direitos fundamentais, nomeadamente, os direitos à intimidade/privacidade, à autodeterminação informacional, à inviolabilidade das comunicações, pois ainda que não seja possível a interceção das comunicações, permite a recolha de dados de tráfego que possam estar no sistema informático alvo de pesquisa, não se olvidando também que na maioria das vezes a pesquisa de dados informáticos implica a entrada numa determinada residência, pelo que o direito à inviolabilidade do domicílio também sofrerá restrições (Nunes D. R., 2018)[28].

Prosseguindo a análise do art.º 15.º, destaca-se o n.º 3, que estabelece as situações em que "*o órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária".*

Assim, nos termos do art.º 15.º, al. a), o OPC pode proceder à pesquisa, *quando a mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado, fique, por qualquer forma documentado.* Nesta situação, o consentimento assume-se como um pressuposto de validade da diligência, sem o qual se estará perante uma prova proibida nos termos do art.º 126.º, n.º 3 do CPP.

Deste modo, há que observar o disposto no art.º 38.º do CP que exige, desde logo, no seu n.º 2, que *o consentimento pode ser expresso por qualquer meio que traduza uma vontade séria, livre e esclarecida do titular do interesse*

[28] Refira-se, a este respeito, que, quando a pesquisa de dados informáticos implique a entrada numa residência, o respetivo mandado de busca e apreensão, emitido pelo JIC, possa prever a pesquisa de dados informáticos. No entanto, ainda assim se entende que a lei deveria ter colocado este meio de obtenção de prova no catálogo de atos a ordenar ou autorizar pelo JIC, atendendo aos direitos fundamentais em causa.

juridicamente protegido. Ora, daqui se depreende que caberá ao OPC que irá realizar a diligência e de quem se espera "uma atitude de respeito pela dignidade das pessoas e da justiça" (Silva, 2000, p. 66), em obediência ao princípio da lealdade, o dever de informar de forma clara e inequívoca o visado acerca do teor da mesma.

Importa previamente precisar que o art.º 15.º, n.º 2, al. a) usa a expressão *por quem tiver a disponibilidade ou controlo desses dados***,** entendendo-se, a este respeito, que a legitimidade para prestar o consentimento será da pessoa que tenha a posse física dos dados informáticos em causa na pesquisa, bem como da pessoa, que não tendo a posse dos mesmos, pode aceder legitimamente ao sistema informático onde estes estão alojados (Nunes D. R., 2018).

Na eventualidade de existirem vários visados numa determinada investigação, todos terão de prestar consentimento para que se possa realizar a pesquisa de dados informáticos (*Ibidem*).

A este respeito, importa destacar a argumentação constante do acórdão do TC 126/2013[29], que, salvo melhor opinião, também aqui deve ser aplicada *mutatis mutandis*:

> (…) perante a intrusão que significa a busca no âmbito de um processo criminal, o consentimento previsto no n.º 3 do art.º 34.º da Constituição tem necessariamente de provir do titular do domicílio que seja visado pela diligência processual (não importa aqui esclarecer se e em que condições esse consentimento além de *necessário* é *suficiente*). Viola a Constituição a norma que considere suficiente, para legitimar a entrada dos órgãos de polícia criminal no domicílio do arguido ou suspeito a fim de realizar uma busca, a permissão conferida por um co-domiciliado com poder de disposição sobre o espaço em causa.

[29] Acessível em: http://www.tribunalconstitucional.pt/tc/acordaos/20130126.html (consultado a 15/04/2020).

Nesta sequência, exigir-se-á também o consentimento ao visado pela pesquisa de dados informáticos, caso tenha a posse física dos mesmos ou, não a tendo, possa legitimamente aceder-lhes. Sendo vários visados, todos terão de prestar consentimento (Nunes D. R., 2018).

Contrariamente, as pessoas que têm a posse física dos dados, ou não a tendo, ainda assim podem legitimamente aceder-lhes, se não forem visados pela investigação, bastará o consentimento de uma delas (*Idem*).

Releva ainda mencionar o art.º 38.º, n.º 3 que estabelece que *o consentimento só é eficaz se for prestado por quem tiver mais de 16 anos e possuir o discernimento necessário para avaliar o seu sentido e alcance no momento em que o presta*. Articulando esta norma, com o disposto no art.º 64.º, n.º 1, al. d) do CPP, importa referir que, no caso da pessoa ser menor de 21 anos, cega, surda, analfabeta, desconhecedora de língua portuguesa, ou se suscitar a questão da sua inimputabilidade ou imputabilidade diminuída é obrigatória a intervenção do defensor para garantir que a pessoa que venha a prestar o consentimento o faça de forma livre e esclarecida[30].

Nos casos em que quem deva prestar o consentimento seja desconhecedor de língua portuguesa, dever-se-á ainda observar o disposto no art.º 92, n.º 2 do CPP, que exige a nomeação de um intérprete.

A não observância destes preceitos legais consubstancia uma nulidade insanável, no caso da não nomeação de defensor, nos termos do art.º 119.º, al. c) conjugado com o art.º 64.º, n.º 1, al. d), ambos do CPP e uma nulidade dependente de arguição no caso da não nomeação de intérprete, *ex vi* art.º 120.º, n.º 2, al. c).

Nos termos do art.º 15.º, n.º 3, al. b), o OPC também pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, *nos casos de terrorismo, criminalidade violenta, ou altamente organizada, quando haja indícios*

[30] A obrigatoriedade de assistência de defensor, nomeadamente, para os casos de menores de 21 anos é abordada no âmbito das buscas domiciliárias, designadamente no âmbito do Ac. RL de 22/01/2019 acedido em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/09b85b00ee0cc22780258397003622cc?OpenDocument&Highlight=0,consentimento,obrigatoriedade,de,defensor (consultado a 14/04/2020).

da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

Para compreender o âmbito desta norma tem de se conjugar a mesma, desde logo, com as definições de terrorismo, criminalidade violenta e altamente organizada, constantes do art.º 1.º, al. i), j) e m) do CPP.

Exige-se ainda *indícios da prática iminente de crime que ponha em grave risco a vida*. Deste modo, a mera suspeita revela-se insuficiente, afigurando-se ainda necessário que a prática criminosa que se visa obviar esteja em execução.

Caso a diligência tenha fundamento na al. b) do art.º 15.º, n.º 3, estabelece o número 4 deste artigo o dever do OPC, que procedeu à sua realização, de comunicar imediatamente à autoridade judiciária competente, sob pena de nulidade, com vista a ser apreciada em ordem à sua validação, bem como de elaborar o relatório previsto no art.º 253.º do CPP.

Em síntese, esta norma apresenta uma dupla vertente de salvaguarda, quer da eficácia de investigação, nos casos da criminalidade mais grave, permitindo às autoridades intervir em casos de *periculum in mora,* quer na proteção de direitos fundamentais da vítima (Nunes D. R., 2018).

Por último, importa ainda referir, seguindo Rui Cardoso, que o DL n.º 137/2019, de 13 de setembro, que aprovou a nova estrutura organizacional da Polícia Judiciária, atribuiu, através do art.º 9.º, n.º 1, al. f), especial competência às autoridades de polícia criminal dessa polícia para, no âmbito de despacho de delegação genérica de competência de investigação criminal, ordenar pesquisa em sistema informático, sempre que não seja possível, dada a situação de urgência e perigo na demora, aguardar pela decisão de autoridade judiciária. Acrescenta ainda este autor que “as autoridades de polícia criminal da Polícia Judiciária têm agora um regime de competência para ordenar pesquisas informáticas bem mais amplo do que as demais” (Cardoso, 2019, p. 66).

Deste modo, atendendo à natureza destas normas, não se pode concordar com o entendimento perfilhado por Benjamim Silva Rodrigues, segundo o qual este tipo de normas “concretiza um verdadeiro direito processual do inimigo” (Rodrigues, 2011, p. 527). Com efeito, as mesmas consubstanciam uma resposta necessária e eficaz aos fenómenos de criminalidade mais grave

suscetíveis de pôr em grave risco a vida de outrem e que, em diversas situações, dificilmente se coadunam com obtenção prévia de uma autorização judicial[31] [32].

Colocando agora o enfoque no art.º 15.º, n.º 5, constata-se que o legislador consagrou uma norma que importa analisar detalhadamente de forma a compreender o seu correto âmbito de aplicação.

Para tal, importa regressar à Convenção sobre o Cibercrime, em concreto à leitura do art.º 19.º, n.º 2 e aos pontos 192 e 195 do respetivo Relatório Explicativo, onde se salienta que a expressão aí constante "no seu território" realça que este meio de obtenção de prova apenas pode ser utilizado no âmbito do território nacional, concluindo-se assim que esta disposição legal *não aborda a busca e apreensão transfronteiriça, que permite aos Estados a possibilidade de realizar buscas e apreensões de dados no território de outras Partes, sem que seja necessário recorrer aos mecanismos de cooperação judiciária internacional*.

No entanto, no capítulo III desta Convenção dedicado à Cooperação Internacional, o art.º 32.º - Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público, admite a possibilidade de se acederem a dados armazenados, seja qual for a sua localização geográfica, desde que os mesmos sejam acessíveis ao público (fonte aberta) ou desde que o acesso seja realizado através do sistema informático situado no seu território e seja obtido o consentimento da pessoa legalmente autorizada a divulgar esses dados.

Por sua vez, o Relatório Explicativo refere no ponto 293 o seguinte:

> Os redatores da Convenção debateram longamente a questão de saber em que circunstâncias deverá ser permitido a uma Parte aceder unilateralmente aos dados informatizados, armazenados no território de uma outra Parte, sem requerer a assistência mútua, concluindo que naquela fase não seria ainda possível elaborar um regime global, legalmente vinculatório que regulamentasse esta

[31] Neste sentido também Duarte Rodrigues Nunes (Nunes D. R., 2018).
[32] Para Guedes Valente a aplicação desta norma deve ser vista à luz do "estado necessidade de intervenção do Estado" (Valente, 2020, p. 149).

> matéria, pelo que apenas seriam definidas no art.º 32.º da Convenção, as situações nas quais, por unanimidade, a ação unilateral se mostrasse aceitável.

Ora, no art.º 15.º n.º 5, o legislador nacional não introduziu nenhuma expressão idêntica que limitasse o âmbito da aplicação da norma aos sistemas informáticos que se encontram em território nacional.

Já no que tange ao art.º 25.º, cuja epígrafe é o Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento, conclui-se que se trata de uma disposição legal, que restringe o acesso transfronteiriço das autoridades estrangeiras aos dados informáticos localizados em Portugal, claramente conforme com a norma do art.º 32.º da Convenção sobre o Cibercrime.

A questão então que importa clarificar é se o art.º 15.º n.º 5 admite estender a pesquisa de dados informáticos aos casos em que os mesmos se encontrem armazenados fora do território nacional, mas legitimamente acessíveis a partir de um sistema informático localizado em Portugal e, caso a resposta seja afirmativa, quais os limites a essa extensão.

A resposta a esta questão, que é defendida pela doutrina, é a de que a Lei do Cibercrime consagrou a possibilidade de realizar pesquisas de dados informáticos em sistemas informáticos, que não se encontram em território nacional, de forma remota e sem recurso à cooperação judiciária internacional, desde que o sistema informático em causa seja acessível através de outro sistema localizado no território nacional[33].

Vejamos, em síntese, os principais argumentos apresentados por Duarte Rodrigues Nunes. Em primeiro lugar, o legislador não restringiu o âmbito de aplicação da norma aos sistemas informáticos que se encontram em território nacional, pelo que essa divergência face ao teor da norma já mencionada constante da Convenção sobre o Cibercrime foi intencional.

[33] *Vide:* Ramalho, 2014, pp. 143-144 e Nunes D. R., 2018, p. 92. Em sentido oposto Rui Soares Pereira, para quem o art. 15.º, n.º 5 não é uma norma habilitante suficiente. Este autor refere ainda que a pesquisa transfronteiriça de dados, de forma unilateral e sem recurso aos mecanismos de cooperação judiciária internacional, a dados armazenados em sistemas localizados no estrangeiro não será conforme no plano das normas ou princípios de direito internacional e, por conseguinte, à CRP (Pereira, 2019, p. 269).

Em segundo lugar, este autor não vê em que medida a pesquisa transfronteiriça de dados, sem recurso à cooperação judiciária internacional, consubstancia uma violação à soberania do Estado, onde se encontram os dados informáticos armazenados, que são objeto de pesquisa.

Em terceiro lugar, o autor refere o facto da criminalidade informática ser tendencialmente aterritorial, salientando-se que para um "cibercriminoso, é tão fácil atacar um alvo nos antípodas como atacar o seu vizinho do lado" (Natário, 2013).

Em quarto lugar, nem sempre é possível determinar em que Estado está situado o sistema informático, onde os dados relevantes para a investigação estão armazenados. Nestes casos, a inadmissibilidade da pesquisa transfronteiriça de dados poderia comprometer o resultado da investigação, salientando-se ainda que os instrumentos de cooperação judiciária internacional são morosos. Ora a Lei do Cibercrime visa precisamente dotar as autoridades de mecanismos eficazes e adequados à prossecução da justiça.

Por sua vez, Silva Ramalho faz a análise desta questão debruçando-se sobre as seguintes situações:

> i. É necessário recolher prova armazenada em servidor estrangeiro, mas acessível ao público;
> ii. A prova encontra-se armazenada em servidor estrangeiro, mas cujo acesso é livremente consentido pela pessoa legalmente autorizada a ceder os dados; ou, por último
> iii. A prova encontra-se armazenada em servidor estrangeiro, mas inacessível ao público e sem a obtenção prévia do consentimento da pessoa autorizada a cedê-la (Ramalho, 2014, p.135).

Relativamente às duas primeiras situações, resulta do que foi exposto anteriormente que as mesmas foram previstas na Convenção sobre o Cibercrime. No ordenamento jurídico nacional, apenas se faz alusão a estas situações no art. 25.º da Lei do Cibercrime, ou seja, para excecionar as

autoridades estrangeiras do pedido prévio às autoridades portuguesas, quando as mesmas se verificarem.

Acerca da admissibilidade da pesquisa transfronteiriça de dados na terceira situação, ou seja, nos casos em que a prova se encontra armazenada em servidor estrangeiro, mas inacessível ao público e sem a obtenção prévia do consentimento da pessoa autorizada a cedê-la, Silva Ramalho também se pronuncia afirmativamente. No entanto, não deixa de levantar questões que, pela sua pertinência, importa ressaltar.

Com efeito, se é verdade que da leitura do art.º 15.º, n.º 5 se conclui que "o legislador português consagrou uma competência territorial irrestrita às autoridades nacionais no que respeita à pesquisa e apreensão remota de dados em sistemas informáticos armazenados em território estrangeiro" (Ramalho, 2014, p. 145), também é evidente que, nos termos do art.º 25.º, tal possibilidade foi vedada às autoridades estrangeiras, que pretendam realizar pesquisas e recolher elementos de prova, que estejam armazenados em território nacional, através dos sistemas informáticos localizados nos seus territórios, salvo quando estes dados estejam publicamente disponíveis ou haja consentimento da pessoa autorizada legalmente a divulgá-los.

Salvo melhor opinião, a não reciprocidade da solução adotada revela-se anacrónica, sendo o exemplo apontado por Silva Ramalho bem ilustrativo dos resultados práticos de tal solução. Com efeito, como bem demonstra este autor, segundo o nosso ordenamento jurídico, o investigador criminal português, no âmbito de uma pesquisa de dados informáticos, poderá, através do sistema informático do suspeito, aceder a um serviço de *webmail*, tal como *Gmail, Outlook ou Yahoo*[34], ou respetivos serviços de armazenamento de dados - *Google Drive, Onedrive,* que se encontrarão alojados nos E.U.A, bastando que, para tal, essas páginas *web* estejam abertas ou as credenciais de acesso se encontrem automaticamente introduzidas nessas páginas.

[34] Também Rui Cardoso refere que o acesso e pesquisa informática às mensagens de correio eletrónico ainda nos fornecedores de serviço de correio eletrónico (*E-mail Service Providers*) foi uma das questões resolvidas pelo art.º 15, n.º 5 e 17.º da Lei do Cibercrime (Cardoso, 2019, p. 68).

Já se o investigador criminal, for por hipótese norte-americano e no âmbito de uma pesquisa de dados informáticos, pretender aceder a um serviço *webmail*, por hipótese SAPO mail ou MEO *Cloud*, cujos servidores estão em Portugal, a partir de um sistema informático localizado nos E.U.A, terá, nos termos do art.º 25.º, al. b) da Lei do Cibercrime, de obter o necessário consentimento. Caso o mesmo não seja prestado, só resta o pedido de cooperação judiciária internacional (*Ibidem*).

A competência territorial irrestrita da pesquisa transfronteiriça de dados informáticos também não se apresenta consentânea com um dos pilares fundamentais da Convenção sobre o Cibercrime que assenta precisamente na criação e respetiva utilização de mecanismos de cooperação internacional, nem com o disposto no art.º 6.º do CPP, que consagra o princípio da territorialidade ou *lex fori*, segundo o qual "os limites da jurisdição criminal coincidem com os limites do território" (Silva, 2000, p. 109).

No entanto, a solução consagrada no art.º 15.º, n.º 5 não deixa de se afigurar conforme com as especificidades inerentes à cibercriminalidade, designadamente o facto de como se referiu anteriormente se tratar de um fenómeno tendencialmente aterritorial, bem como no que diz respeito à recolha de prova digital, salientando-se aqui a sua fragilidade e suscetibilidade de dispersão. Atualmente, encontra-se generalizada a utilização de redes sociais, serviços de *webmail,* bem como de armazenamento de dados na *cloud,* que se encontram alojados fora do território nacional, muitas das vezes desconhecendo-se efetivamente o local concreto onde os mesmos se encontram armazenados. Além do mais, estes serviços apresentam como uma das principais vantagens a sincronização imediata de dados nos vários dispositivos utilizados por um determinado utilizador.

Deste modo, se a pesquisa de dados informáticos não fosse levada a cabo no imediato pelas autoridades, ainda que fosse apreendido o computador e o telemóvel utilizados pelo suspeito, este, por exemplo, ou outra pessoa que conhecesse as credenciais de acesso, poderia aceder a partir de outro dispositivo aos serviços onde os dados se encontram armazenados e proceder à sua eliminação.

Assim, a possibilidade da extensão da pesquisa de dados informáticos tal como consagrada na Lei do Cibercrime destaca-se pelo caráter inovador, cuja teleologia radica precisamente em razões de eficácia na recolha de prova digital.

1.4.5. A APREENSÃO DE DADOS INFORMÁTICOS

A apreensão "é o meio de obtenção de prova que se destina a colocar à disposição do processo, tornando-o indisponível para o proprietário ou detentor" (Marcolino de Jesus, 2019, p. 252) *os objetos que tiverem servido ou estivessem destinados a servir a prática de um crime, os que constituírem o seu produto, lucro, preço ou recompensa, e bem assim todos os objetos que tiverem sido deixados pelo agente no local do crime ou quaisquer outros suscetíveis de servir de prova* – art.º 178.º, n.º 1 do CPP.

Nos termos do art.º 19.º da Convenção sobre o Cibercrime faz-se referência à apreensão ou à obtenção de forma semelhante dos dados informáticos relativamente aos quais o acesso foi realizado na sequência da realização de buscas, evidenciando-se que nos termos do ponto 197 do Relatório Explicativo da Convenção:

> O termo "apreender" significa transportar para fora do local em questão, o suporte físico no qual foram registados os dados ou as informações. O termo "apreender" inclui, ainda, a utilização ou apreensão de programas necessários para aceder aos dados objeto de busca e investigação (…). Uma vez que as medidas instituídas se referem aos dados intangíveis armazenados, torna-se necessário que as autoridades competentes adotem as medidas complementares no sentido da aquisição e guarda de dados, isto é, de maneira a "preservar a integridade dos dados", ou manter a cadeia de posse dos dados o que significa que os dados copiados ou removidos são conservados no estado em que forem encontrados aquando da apreensão, mantendo-se inalterados no

> período durante o qual é intentada a ação penal. A expressão remete-nos, pois, para um assumir do controlo dos dados ou para a remoção dos mesmos do local em questão.

De acordo com a Lei do Cibercrime a apreensão de dados informáticos "consiste em as autoridades obterem, para o processo, dados informáticos que se encontrem num sistema informático ou suporte autónomo que tenha sido alvo de uma pesquisa informática ou de outro acesso legítimo e que sejam necessários à descoberta da verdade material e/ou para a prova" (Nunes, 2018, p. 117).

Assim, quando no decurso de uma pesquisa informática ou de outro acesso legítimo forem encontrados elementos de prova com interesse para a investigação, dispõe o art.º 16.º, n.º 1, que a autoridade judiciária competente autoriza, ou ordena, por despacho, a apreensão dos mesmos.

Salienta-se ainda o n.º 2 deste artigo, segundo o qual também o órgão de polícia criminal pode efetuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de uma pesquisa informática legitimamente ordenada e executada nos termos do n.º 1, bem como quando haja perigo na demora.

O n.º 3 estabelece a exigência de apresentar ao juiz os dados ou documentos informáticos apreendidos, cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do titular ou do terceiro, sob pena de nulidade. Caberá ao juiz ponderar a sua junção aos autos tendo em conta os interesses do caso concreto.

No âmbito deste artigo, assume especial relevância o estabelecido no n.º 7 salientando-se que a apreensão de dados informáticos poderá revestir diversas formas, tal como previsto na Convenção sobre o Cibercrime, designadamente *a apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como os dispositivos necessários à respetiva leitura* (art.º 16.º n.º 7, al. a) e a *realização de uma cópia de dados, em suporte autónomo, que será junto ao processo* (art.º 16.º n.º 7, al. b), o que poderá ser efetuado com recurso a ferramentas forenses adequadas que garantam a integridade da prova. Neste

último caso, dispõe o n.º 8, que se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital. A práxis policial sujeita a cópia à função *hash (digital fingerprint*)*, "*que utiliza um algoritmo que calcula a soma binária dos dados apresentados à função, retornando uma sequência de *bits* de comprimento fixo em numeração hexadecimal" (Antunes & Rodrigues, 2018, p. 159)*.*

Desse modo, quando as ferramentas forenses copiam ou extraem os dados dos dispositivos eletrónicos, gravam o *hash* dos ficheiros e da imagem da memória obtida. Posteriormente poder-se-á utilizar esses algoritmos para efetuar uma verificação comparativa de forma a confirmar que nada foi alterado desde a cópia/extração realizada, sendo uma boa prática realizar uma verificação do *hash* antes e depois do exame de forma a garantir, de forma inequívoca, a custódia da prova (Ramos, 2014). É sobre esta cópia que deverá incidir a análise do conteúdo com vista a localizar os elementos de prova com interesse para uma determinada investigação criminal, assegurando-se, deste modo, que a prova original se mantém inalterada (Antunes & Rodrigues, 2018).

Este regime da apreensão de dados informáticos não se poderá confundir com o facto de, não raras vezes, no decurso de investigações, se apurarem informações livremente acessíveis e com relevância probatória em plataformas na internet. Com efeito, como se refere no Acórdão da Relação do Porto de 5 de abril de 2017, "em processo penal, nada impede a impressão de informação livremente acessível a todos, no *Facebook*, ou noutra plataforma de internet"[35].

1.4.6. A APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÕES DE NATUREZA SEMELHANTE

Relativamente à apreensão de correio eletrónico e registos de comunicações de natureza semelhante, haverá que ter em atenção o disposto no art.º 17.º da Lei do Cibercrime, que manda aplicar *correspondentemente o regime da apreensão de correspondência previsto no CPP*.

[35] Acessível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/16ebc99e65fc19038025810c0051991a?OpenDocument (Consultado a 28/06/2020).

Esta norma específica, como refere Duarte Rodrigues Nunes e Rita Castanheira Neves, é inexistente na Convenção sobre o Cibercrime (Neves, 2011, p. 273), tratando-se de uma criação do legislador português (Nunes D. R., 2018).

Antes de proceder à análise deste regime legal, cumpre desde logo destacar que se pode encontrar uma definição legal de correio eletrónico no art.º 2.º, n.º 1, al.) b) da Lei 41/2004, de 18 de agosto, que regula a proteção de dados pessoais e privacidade nas telecomunicações. Assim, correio eletrónico é *qualquer mensagem textual, vocal, sonora, ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha*.

Dias Ramos define correio eletrónico do seguinte modo:

> Um programa informático que permite a comunicação instantânea, de modo diferido, entre quem envia e quem a recebe, através das redes de informação e comunicação, independentemente do local em que estes se encontrem, sem a necessidade deste se encontrar instalado no computador (Ramos, 2014, p. 28).

No que concerne às comunicações de natureza semelhante, a doutrina e a jurisprudência têm vindo a incluir outros meios de comunicação com uma grande expressão, atualmente, tais como os serviços de mensagens curtas - *SMS* (Dá Mesquita, 2010, p. 119) e *MMS*, que muito em breve serão substituídos pelos *RCS* (*Rich Communication Services*) *Facebook Messenger, WhatsApp, Skype*, entre outros (Nunes D. R., 2018, p. 140).

A evolução nesta área tem sido notável, salientando-se que os RCS[36], numa tentativa de acompanhar as aplicações de comunicação instantâneas apresentam funcionalidades idênticas, destacando-se o envio de vídeos, a possibilidade de saber quando uma mensagem foi lida pelo destinatário, saber

[36] Mais informação sobre o *RCS* pode ser consultada em: https://pplware.sapo.pt/smartphones-tablets/adeus-sms-rcs-chegou-aos-clientes-nos-nowo-e-meo/ (consultada a 28/06/2020).

quando o destinatário está a escrever a mensagem, a criação de grupos e, em breve, a encriptação[37].

Iniciando a análise do regime legal, no que tange à apreensão de correio eletrónico e registos de natureza semelhante, cumpre desde logo fazer uma distinção entre as comunicações que se encontram armazenadas no sistema informático acedido pelos OPC e as que decorrem em tempo real.

Neste seguimento, evidencia-se que o âmbito da aplicação da norma constante do art.º 17.º da Lei do Cibercrime diz respeito a correio eletrónico ou registos de comunicações de natureza semelhante que estejam armazenados no sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro e que tenham sido encontrados no decurso de uma pesquisa informática ou outro acesso legítimo, excluindo-se deste modo a obtenção destas comunicações em tempo real.

Exclui-se também do âmbito desta norma, o consentimento prestado por uma pessoa para que as autoridades se inteirem do teor de determinado correio eletrónico ou de determinadas comunicações de natureza semelhante e, nessa sequência, essas comunicações venham a ser juntas aos autos[38].

A apreensão nos termos desta norma só é possível se for ordenada ou autorizada pelo juiz e esta seja de grande interesse para a descoberta da verdade ou da prova, *aplicando-se correspondentemente o regime de apreensão de correspondência previsto no CPP*.

No que concerne à remissão do art.º 17.º para o art.º 179.º do CPP, constata-se que tem sido objeto de diversas críticas por parte da doutrina, como adiante se verá.

Porém, salienta-se desde logo que é inaplicável ao correio eletrónico e aos registos de comunicações de natureza semelhante a exigência de crime punível com pena de prisão superior, no seu máximo, a 3 anos (*Vide* art.º 179.º, n.º 1, al. b), porquanto resulta da conjugação do art.º 11.º com o art.º 17.º da Lei

[37] https://www.noticiasaominuto.com/tech/1490202/app-de-mensagens-da-google-tera-encriptacao (Notícia de 25/05/2020 e consultada a 28/06/2020).

[38] *Vide* a este respeito o Ac. da RL de 29/03/2012 a propósito da junção aos autos da transcrição das mensagens *SMS* gravadas no telemóvel do queixoso, depois do consentimento deste (Consultado a 28/06/2020). No mesmo sentido o Ac. da RP de 22/05/2013.

do Cibercrime, que a apreensão de correio eletrónico e registos de comunicações de natureza semelhante é um meio de obtenção de prova suscetível de ser utilizado nos crimes previstos nesta lei, cometidos por meio de um sistema informático e em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (Neves, 2011, pp. 274- 275) .

Cumpre ainda referir que, segundo Rita Castanheira Neves, deverão ser observados quatro aspetos desta norma legal: a cominação da nulidade, no caso do não respeito pelos requisitos estabelecidos; o facto de estar em causa correio eletrónico e registos de comunicações de natureza semelhante enviado ou recebido pelo suspeito mesmo que de/a partir de endereço eletrónico de pessoal diversa, conforme estabelece a al. a) do n.º 1 do art.º 179.º; a proibição, sob pena de nulidade, da apreensão de correio eletrónico e registos de comunicações de natureza semelhante trocados entre o arguido e o defensor, salvo se o juiz tiver fundadas razões para crer que estes constituem objeto ou elemento de um crime – n.º 2 do art.º 179.º; e, o facto de ter que ser o juiz que tiver autorizado ou ordenado a diligência a primeira pessoa a tomar conhecimento do conteúdo do correio eletrónico e dos registos de comunicações de natureza semelhante, ordenando a sua junção aos autos, caso considere relevante para a prova; caso contrário, deve mandar restituir a quem de direito, não podendo ser utilizados como meio de prova, ficando ainda o juiz vinculado ao dever de segredo relativamente ao que tiver tomado conhecimento - art.º 179.º, n.º 3 (Neves, 2011, pp. 274-275).

No que tange a este aspeto tem vindo a ser referido pela doutrina que esta norma legal permite a apreensão provisória de correio eletrónico e registos de comunicações de natureza semelhante, no âmbito de pesquisas realizadas na sequência de autorização do Ministério Público, devendo estes ser presentes ao juiz a fim de ordenar a respetiva apreensão e junção aos autos (Verdelho, 2009, p. 744).

Pedro Verdelho pronuncia-se ainda no sentido de não se exigir que seja o juiz o primeiro a ter conhecimento de todas as mensagens, apontando, ao invés, a possibilidade de quem procede à pesquisa encaminhar para o juiz mensagens concretas, com relevância para o caso concreto, que aquele depois

apreenderá ou não. Com efeito, não sendo este o entendimento, refere o autor que se estaria a optar por uma "solução processual inviável que exigiria a verificação, pelo juiz, de todas as mensagens de correio eletrónico, em todos os computadores que fossem encontradas no decurso de pesquisas" (*Ibidem*).

Também neste sentido Pica dos Santos refere que sempre que possível, "a melhor solução será a de admitir uma primeira seleção das mensagens relevantes por quem executa a busca, atendendo, designadamente, à data das mensagens, ao remetente e/ou destinatário, bem como aos dados/informações já constantes do processo" (Pica dos Santos, pp. 252-253). O resultado desta seleção será submetido ao juiz, com vista a tomar conhecimento do teor integral das mensagens, evitando-se assim uma "indesejável apreensão massiva de e-*mails*." (*Ibidem*).

Não admitir esta possibilidade exigiria que os investigadores, quando realizassem pesquisas informáticas, fossem, à cautela, acompanhados pelo JIC ou, logo que detetassem a existência de correio eletrónico teriam de o contactar para este se deslocar ao local (Rodrigues Nunes, 2018). Poderiam ainda apreender e transportar os computadores, para o JIC poder visualizar os *e-mails*. No entanto, esta solução afigura-se inexequível atendendo, desde logo, ao elevado número de buscas e pesquisas informáticas realizadas pelos OPC[39].

Deste modo, "o procedimento habitual consiste na realização de uma imagem do suporte físico apreendido (disco rígido, *pen* USB, outro) e é a partir desta imagem (ou clone – sendo esta a expressão mais apropriada) que se vai desenrolar todo o procedimento pericial" (Ramos, 2014, p. 94).

Para a realização desta imagem e com vista a garantir a custódia da prova recorre-se, desde logo, a um bloqueador de escrita, o que evita a adulteração dos dados apreendidos e a ferramentas forenses produzidas *ad hoc*.

No âmbito da pesquisa de dados informáticos, ao realizar a triagem forense, com vista a aferir a existência de elementos de prova com interesse para uma determinada investigação, com base nestas ferramentas informáticas,

[39] Sobre estas dificuldades já Rogério Bravo havia alertado em 2006 (Bravo, 2006).

é frequente, desde logo por questões de celeridade, recorrer à pesquisa por palavras-chave.

No entanto, como explica Dias Ramos "a ferramenta forense não vai conseguir destrinçar o que é correio eletrónico daquilo que efetivamente não o é. Esta pesquisa por palavras-chave apenas vai coligir dados informáticos, tendo por base o sistema binário" (*Ibidem*). Só em momento posterior, quando o perito procede à análise desses dados é que se poderá deparar com correio eletrónico, devendo extrair essas mensagens e gravá-las num suporte adequado a fim de as remeter ao JIC para que possa tomar conhecimento e ordenar a sua junção aos autos.

Sendo certo que as posições doutrinárias anteriormente referidas se afiguram mais consentâneas com as necessidades de investigação criminal, a verdade é que, a jurisprudência não as acolheu. Com efeito, o Tribunal da Relação de Lisboa, no seu acórdão de 6 de fevereiro de 2018[40] e mais recentemente no de 4 de fevereiro de 2020[41], refere que compete exclusivamente ao juiz de instrução tomar conhecimento, em primeira mão do conteúdo da correspondência apreendida, o que se aplica ao correio eletrónico já convertido em ficheiro legível, constituído a sua violação uma nulidade expressa absoluta.

Evidencia-se ainda este último acórdão, desde logo pelo facto de apresentar uma perspetiva cronológica do que vem sendo o entendimento jurisprudencial do Tribunal na Relação de Lisboa nesta matéria, sendo certo que não foram encontradas decisões sobre esta matéria específica proferidas pelos outros Tribunais da Relação.

[40] Acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument (Consultado a 26/07/2020).
[41] Acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a411de057cfd2e1d80258507004c7e4e?OpenDocument&Highlight=0,art,17,lei,do,cibercrime (Consultado a 26/07/2020).

Com efeito, já no âmbito do acórdão do TRL de 11/01/2011 se referia que o art.º 17.º, ao remeter para o regime geral previsto no CPP, implicava a sua aplicação na totalidade, ou seja, sem redução do seu âmbito[42].

No seguimento do acórdão anterior, também no acórdão de 06/02/2018 resulta clara a aplicação da norma legal prevista no art.º 179.º n.º 3 do CPP ao correio eletrónico e registos de comunicações de natureza semelhante, que estabelece que *o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo*, salientando ainda que este ato processual é um ato obrigatório da competência exclusiva do juiz de instrução, nos termos do art.º 268.º, n.º 1, al. d) também do CPP. Deste modo, em caso de inobservância destas normas legais, estar-se-ia perante uma nulidade prevista no art.º 120.º, n.º 2, al. d) do CPP.

Em análise a este acórdão, Duarte Rodrigues Nunes apresenta um conjunto de argumentos que justificarão, segundo a sua perspetiva, que o regime de apreensão de correspondência previsto no CPP deverá ser aplicado "*cum grano salis e mutatis mutandis* à apreensão de correio eletrónico e registos de natureza semelhante" (Rodrigues Nunes, 2018, p. 38), concluindo que "existirão aspetos do regime de correspondência que não são aplicáveis à apreensão de correio eletrónico e registos de natureza semelhante ou sendo-o, não o são nos mesmo termos em que são aplicáveis à apreensão de correspondência tradicional" (*Ibidem*).

Na verdade, o regime de apreensão de correspondência previsto no CPP é um meio de obtenção de prova com requisitos mais exigentes face ao regime geral das apreensões pelo facto de estar em causa, além do direito à reserva da vida privada, também o direito à inviolabilidade da correspondência tutelado diretamente pelo art.º 34.º da CRP. Compreende-se tais exigências dado que a apreensão de correspondência "consiste na retirada do circuito normal do correio do suporte através do qual se efetua uma comunicação postal ou telegráfica, impedindo que chegue ao seu destinatário" (Rodrigues Nunes,

[42] Acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument (Consultado a 26/07/2020).

2018, p. 27), ou seja, “esta disposição protege toda a correspondência enquanto ela não for aberta pelo seu destinatário” (Albuquerque, p. 494).

Ora, o âmbito de aplicação do art.º 17.º da Lei do Cibercrime é a obtenção de mensagens de correio eletrónico e registos de comunicações de natureza semelhante que já foram recebidas pelo destinatário.

Caso se visasse a obtenção desses dados em tempo real teria que se observar o disposto no art.º 18.º dessa lei que respeita à interceção de comunicações.

Deste modo, a apreensão de correio eletrónico e registos de comunicações de natureza semelhante não beliscará o direito à inviolabilidade da correspondência, como sucede nos casos previstos no art.º 179.º do CPP.

Outro dos argumentos apresentados pelo autor resulta do facto dos dados informáticos de cariz pessoal ou íntimo estarem sujeitos ao disposto no art. 16.º n.º 3 da Lei do Cibercrime, exigindo-se, sob pena de nulidade, que os mesmos sejam apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto, o que pressupõe um conhecimento prévio da natureza desses dados por parte dos OPC e, no caso do correio eletrónico ou de registos de comunicação de natureza semelhante, cujo conteúdo possa ser menos sensível, ter que se aplicar um regime ainda mais exigente, em que se torna necessário ser o juiz que tiver autorizado ou ordenado a diligência a primeira pessoa a tomar conhecimento desses dados apreendidos.

Outra das incongruências apontadas, prende-se precisamente com as diferenças de regime para os casos em que a correspondência física é aberta e lida pelo destinatário com os casos em que, por exemplo, o correio eletrónico é também aberto e lido pelo destinatário. Tratando-se de correspondência física, depois de aberta pelo seu destinatário, torna-se um mero documento e está sujeita ao regime geral da apreensão (Albuquerque, 2008, p. 494). Caso se trate de correio eletrónico ou por exemplo uma mensagem de *Whatsapp* aberta e lida pelo destinatário, será de aplicar, ainda assim, o regime da apreensão da correspondência.

Aos argumentos apresentados acresce um de cariz prático, a que já se fez alusão anteriormente e havia sido mencionado por Pedro Verdelho e Pica dos Santos, que é a dificuldade do juiz, na fase de inquérito, conseguir selecionar de forma expedita quais os *e-mails* ou mensagens de plataformas instantâneas que são relevantes no meio de centenas ou milhares.

Duarte Rodrigues Nunes conclui assim que o art.º 17.º da Lei do Cibercrime deveria ser revogado, devendo aplicar-se à apreensão de correio eletrónico e registos de comunicações de natureza semelhante o regime previsto no art.º 16.º dessa lei, evidenciando que o n.º 3 desse artigo constitui "uma salvaguarda suficiente para a proteção da intimidade/privacidade" (Rodrigues Nunes, 2018, p. 37).

De iure condito, defende este autor, que se "deverá interpretar o art.º 17.º de forma hábil, apenas sendo aplicável nos casos em que o *e-mail, sms, mms*, etc, ainda não tenham sido abertos pelo destinatário" (*Ibidem*).

No entanto e, prosseguindo com as referências jurisprudenciais, sublinha-se que também no acórdão do TRL de 07/03/2018[43] pode ler-se que:

> Não esteve no espírito do legislador transpor para o correio eletrónico e registos de natureza semelhante a distinção, por referência ao correio tradicional, de correio aberto ou fechado, o que desde logo se colhe do elemento literal previsto nesse preceito legal (art.º 17.º) com a expressão "armazenados" o que pressupõe que a comunicação já foi recebida/lida e, consequentemente armazenada, além de não existirem razões para considerar diminuídas as exigências garantísticas do correio eletrónico quando aberto/lido relativamente ao correio eletrónico fechado, atenta à natureza própria destas comunicações.

O acórdão do TRL de 4 de fevereiro de 2020 afigura-se ainda relevante por claramente se distanciar das posições doutrinárias que confluem no sentido da não obrigatoriedade de ser o juiz de instrução criminal o primeiro a tomar

[43] Acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a411de057cfd2e1d80258507004c7e4e?OpenDocument (Consultado a 26/07/2020).

conhecimento do correio eletrónico apreendido. Estriba esta posição no facto do legislador ter valorado sobretudo a natureza de "correspondência" e não tanto a sua natureza eletrónica, pelo que não faria sentido consagrar uma menor proteção à correspondência eletrónica. Refere ainda o facto de o critério mais adequado à interpretação das normas restritivas de direitos fundamentais ser aquele que "assegure a menor compressão possível dos direitos afetados", salientando o facto de se estar no domínio de "eventuais proibições de prova".

Por último, salienta ainda a possibilidade do JIC poder ser assessorado tecnicamente na seleção de mensagens com interesse para a descoberta da verdade ou para a prova, mitigando-se assim a circunstância de não ter o domínio do inquérito.

Chegado a este ponto e depois de apresentadas as especificidades do regime legal da apreensão do correio eletrónico e registos de comunicações de natureza semelhante, bem como as posições doutrinárias e os mais recentes acórdãos do Tribunal da Relação de Lisboa sobre esta temática, importa ainda referir a posição defendida por Dias Ramos que vai no sentido de se alterar o art.º 17.º de forma a que o correio eletrónico passe a ser tratado apenas como um ficheiro informático (Ramos, 2014, p. 113).

Refere este autor que uma mensagem de correio eletrónico não é mais do que um ficheiro digital e que quando se realiza um exame forense após a apreensão de dados informáticos as ferramentas forenses não conseguem distinguir se se está perante correio eletrónico (*Ibidem*). Este argumento de ordem prática associado ao facto de ser cada vez mais frequente a utilização de serviços de *webmail*, cujos conteúdos se encontram alojados na nuvem, permitindo ao utilizador aceder à informação de forma remota e sincronizada a partir de qualquer equipamento informático (*Idem*, p. 110) levanta ainda mais dificuldades aos OPC na apreensão desses dados.

Não existindo a possibilidade de exportar cópia do conteúdo de uma determinada caixa de correio eletrónico como sucede por exemplo na conta Google, através do *Google Takeout*[44], a questão que se impõe é se é aplicável

[44] Sobre o *Google Takeout*: https://support.google.com/accounts/answer/3024190?hl=en. No que diz respeito a plataformas de comunicação instantânea, constata-se que, por exemplo, o

o art.º 16.º n.º 7, al. e) – bloqueio de acesso aos dados. Para tal, após colaboração do visado no fornecimento da *password*, terá de se proceder à alteração da mesma, alterando-se ainda o modo como o acesso à conta pode ser recuperado. Posteriormente, o juiz de instrução criminal poderá aceder ao *webmail*, analisar as mensagens constantes do mesmo e decidir as que deverão ser juntas aos autos (Ramos, 2014). Esta solução comporta sempre o risco de o suspeito poder, de alguma forma, recuperar o acesso à conta e eliminar mensagens que possam ser relevantes para determinada investigação.

A solução para estes casos implicaria o JIC acompanhar estas diligências realizadas pelos OPC, tomando conhecimento do teor do correio eletrónico do suspeito e das comunicações do mesmo de forma a poder selecionar as que se afigurassem com relevância para a descoberta da verdade ou para a prova.

Todavia em termos práticos, como se referiu, será inexequível. E o que é certo é que não temos dúvidas que a interpretação que vem sendo preconizada pelo Tribunal da Relação é a que efetivamente se pode extrair do regime legal vigente, com todas as incongruências apontadas pela doutrina e dificuldades sentidas pelos OPC no âmbito das investigações que levam a cabo.

Deste modo, urge proceder à alteração ou revogação do art.º 17.º da Lei do Cibercrime no que tange à apreensão do correio eletrónico e registos de comunicações de natureza semelhante, aplicando-se aos mesmos o disposto no art.º 16.º, n.º 3 dessa lei, assegurando que todos esses elementos suscetíveis de servir de prova seriam presentes, *a posteriori*, ao juiz para que o mesmo decida a sua junção aos autos, após uma prévia seleção efetuada pelos OPC, afastando-se assim de forma inequívoca a remissão para o art.º 179.º do CPP.

Facebook também permite fazer uma exportação dos dados, incluindo das conversações, para mais informação poderá ser consultado o *site*: https://pt-pt.facebook.com/help/930396167085762. Os *sites* referidos foram consultados a 11/08/2020.

1.4.7. A INTERCEÇÃO DE COMUNICAÇÕES

A interceção de comunicações é um meio de obtenção de prova que se encontra previsto no art.º 18.º da Lei do Cibercrime e que tem a sua origem nos artigos 20.º e 21.º da Convenção sobre o Cibercrime, cujas epígrafes são "Recolha em tempo real de dados relativos ao tráfego" e "Interceção de dados relativos ao conteúdo".

Evidencia-se que o conceito de interceção consta do art.º 2.º al. e) da própria Lei do Cibercrime como sendo o *ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos e outros.*

Cumpre também ressaltar que, diversamente do que sucede com os meios de obtenção de prova previstos nos artigos 12.º a 17.º da Lei do Cibercrime, a interceção de comunicações e as ações encobertas, que veremos de seguida aplica-se a um âmbito muito mais restrito de ilícitos criminais. Tal deve-se à proteção constitucional da inviolabilidade das comunicações.

Começar-se-á por analisar o âmbito de aplicação deste meio de obtenção de prova com a citação da explicação constante do Acórdão do Tribunal da Relação de Évora de 20/01/2015:

> Na Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11.º a 17.º e o regime dos artigos 18.º e 19.º do mesmo diploma. O regime processual dos artigos 11.º a 17.º surge como o regime processual «geral» do cibercrime e da prova eletrónica. Isto porquanto existe um segundo catálogo na Lei n.º 109/2009, o do artigo 18.º, n.º 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18.º e 19.º - são aplicáveis por remissão expressa os artigos 187.º, 188.º e 190.º do CPP e sob condição de não contrariarem e Lei 109/2009 (…). A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos

> artigos 12.º a 17.º se referirem à pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18.º do diploma se refere à interceção de comunicações eletrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático[45].

Conforme se alcança deste acórdão, o art.º 18.º diz sempre respeito a uma interceção de comunicação em tempo real, ou seja, em transmissão, ao invés dos meios de obtenção de prova já analisados, tais como a injunção ou a pesquisa de dados informáticos que se reporta a dados armazenados (Neves, 2011).

Estabelecida esta diferenciação, da análise do art.º 18.º, n.º 1, al. a) e b) constata-se que este meio de obtenção de prova pode ser utilizado relativamente aos crimes previstos na Lei do Cibercrime ou crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no art.º 187.º do CPP.

A questão que inevitavelmente se tem de colocar é a de como se deve delimitar o âmbito de aplicação deste artigo face às interceções telefónicas, meio de obtenção de prova este que se encontra previsto no referido art.º 187.º do CPP. Com efeito, como é sublinhado no Relatório Explicativo da Convenção do Cibercrime, tem-se vindo a assistir a uma "convergência das tecnologias da informação e das telecomunicações, tornando-se pouco nítida a distinção existente entre as telecomunicações e as comunicações informáticas".[46] A doutrina parece apresentar algum consenso no que concerne ao âmbito dos dados de conteúdo, abrangendo a interceção de comunicações informáticas, em tempo real nomeadamente de correio eletrónico, bem como as conversações através de internet utilizando programas específicos para esse efeitos,

[45] http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument (Consultado a 27/09/2020).
[46] *Vide* ponto 206 do Relatório Explicativo da Convenção do Cibercrime.

destacando-se a título de exemplo o *Whatsapp, o Viber, Telegram, Skype, Google Hangouts, Facebook Messenger*, entre outros (Nunes D. R., 2018).

Trata-se, portanto, de um importante meio de obtenção de prova, face à nova realidade tecnológica, salientando-se que estes programas permitem muitas funcionalidades de comunicação que vão desde a troca de mensagens escritas e conversação por voz à realização de videochamadas e partilha de vídeos e documentos. Muitas destas aplicações, como se verá, caracterizam-se ainda por garantir comunicações seguras, através da encriptação de dados, pelo que a interceção, para ser bem-sucedida, terá de ocorrer antes desse processo de encriptação (*Idem*, p. 157).

Relativamente aos requisitos para a utilização deste meio de obtenção de prova, estabelece o n.º 2 do art.º 18.º que a *diligência seja indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter*. Trata-se de um meio de *ultima ratio*, devido ao seu caráter altamente lesivo dos direitos fundamentais. Deste modo, a sua utilização só é justificável, quando um meio de obtenção de prova menos gravoso não permitir a obtenção dos resultados que se procuram atingir (*Idem*, p. 177). Exige-se ainda que o recurso à interceção de comunicações dependa da autorização do JIC.

O regime da interceção e gravação das comunicações segue o disposto nos artigos 187.º, 188.º e 190.º do CPP, respeitante às escutas telefónicas.

1.4.8. AS AÇÕES ENCOBERTAS

O art.º 19.º da Lei do Cibercrime diz respeito às ações encobertas, tendo a doutrina vindo-se a referir a este meio de obtenção de prova como ações encobertas em ambiente digital (Nunes, 2018).

Não existe qualquer norma idêntica na Convenção do Cibercrime, mas o fundamento da consagração deste inovador meio de obtenção de prova residirá no reconhecimento da "necessidade de recurso a métodos de investigação criminal mais agressivos em relação a uma criminalidade que tem beneficiado largamente da ineficácia dos restantes meios disponíveis" (Ramalho, 2013 p. 407-408).

A este respeito salienta-se que, de acordo com o art.º 19.º n.º 1, al. a) e b), este meio de obtenção de prova poderá ser utilizado nos crimes previstos na Lei do Cibercrime, ou ainda *quando cometidos por meio de um sistema informático, quando lhes corresponda em abstrato, pena de prisão superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual no casos em que os ofendidos sejam menores ou incapazes, a burla qualificada e as comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos*. "Ao reduzir o seu objeto a cibercrimes, muitas das vezes de gravidade média ou com penas relativamente baixas, a norma traz implícito um juízo de dificuldade acrescida na obtenção de prova" (Ramalho, 2017, p. 303).

Trata-se, no entanto, de um meio também de *ultima ratio*, o que significa que só se pode recorrer ao mesmo nos casos em que outros meios menos lesivos de direitos se revelem insuficientes para alcançar o resultado que se visa atingir (Nunes, 2018). A título de exemplo dir-se-á que os outros meios de obtenção de prova serão insuficientes, quando os crimes ocorrem na *Darknet* e os seus autores dissimulam o seu endereço IP, através da utilização de programas informáticos de navegação na internet específicos, tais como o TOR *browser,* inviabilizando-se assim a identificação do titular da ligação à internet (Ramos, 2015).

A definição de ação encoberta consta do art.º 1.º n.º 2 da Lei 101/2001 - Regime jurídico das ações encobertas para fins de prevenção e investigação criminal, que refere serem *aquelas desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade.*

A especificidade da ação encoberta em ambiente digital, integra a participação em *chats*, *websites, blogs* ou fóruns, livremente acessíveis ou de acesso reservado, utilizando uma identidade fictícia, "ganhando a confiança dos visados, mantendo-se a par dos acontecimentos e acompanhando a execução dos factos, interagindo com outros participantes (…) e praticando atos

preparatórios ou mesmo de execução (caso tal se mostre necessário), mas sem determinar ninguém à prática de infrações" (Nunes, 2018, p. 198-199).

Duarte Rodrigues Nunes e Silva Ramalho referem que, caso o agente participe nesses *chats, websites ou blogs* sem interagir, limitando-se a visionar os conteúdos ilícitos que vão sendo partilhados (por exemplo de pornografia infantil) e a recolher informação quanto a essa plataforma e utilizadores ativos então neste caso não será de aplicar o regime da ação encoberta[47]. Este último autor enquadra esta atividade naquilo a que doutrina espanhola designa de *Ciberpatrulhaje* exigindo a verificação das seguintes condições: livre acessibilidade do *website*, ainda que mediante um registo prévio formal; recurso, por parte do agente, a um nome de utilizador neutro e sem relação com o conteúdo do site em causa; não interação com os outros utilizadores; a imediata comunicação de indícios da prática de ilícitos de natureza criminal para início formal de inquérito, quando não haja um em curso; frequência exclusiva de *websites* nos quais haja suspeitas da prática de ilícitos; registo das comunicações apenas quando criminalmente relevantes (Ramalho, 2017, p. 297).

A utilização da identidade fictícia ocorrerá quando se cria um perfil falso ou um *username* para interagir com terceiros, não sendo, por norma, aplicável o art. 5.º da Lei n.º 101/2001 (*Idem*).

Não obstante não ser objeto do presente estudo a análise das posições doutrinárias que distinguem agente encoberto de agente infiltrado e de agente provocador[48], cumpre evidenciar que esta é uma das questões que poderá suscitar dificuldades no âmbito das especificidades deste meio de obtenção de prova em ambiente digital, pelo seu caráter altamente lesivo de direitos, salientando-se as questões/exemplos apresentadas por Silva Ramalho se pode ser considerado provocador o agente que entra num *chat* frequentado por pedófilos, que trocam informações de como seduzir crianças, e aí se apresenta com o *nickname 12yearoldgirl*? Ou o agente que entra num *chat* onde sabe

[47] (Nunes D. R., 2018, p. 198); (Ramalho, 2017, p. 297).

[48] Para esta distinção *vide*: Acórdão da Relação de Lisboa de 22/03/2011, acessível em http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/e324710ede9b8ed88025788b00345015?OpenDocument (consultado a 20/09/2020).

poder-se adquirir droga com o *nickname lookingforcocaine* (Ramalho, 2017, p. 296)? Não serão estes *nicknames,* em especial o último, *de per si* provocadores?

Face a estas questões, conclui Silva Ramalho, que "à falta de desejável disposição legal específica, a autorização da autoridade judiciária deve incluir referência expressa aos limites à criação de nomes excessivamente sugestivos, mas também prevendo a possibilidade de, no perfil falso, ser introduzida uma fotografia de outrem" *(Ibidem*, p. 306).

A ação encoberta em ambiente digital constitui um importante recurso no combate a diversos tipos de criminalidade, salientando-se a pornografia infantil e o tráfico de estupefacientes. As suas principais vantagens assentam na possibilidade de identificação dos autores dos ilícitos criminais, bem como da sua localização e obtenção de ficheiros relevantes suscetíveis de servir de prova (Ramalho, 2013).

Por último, salienta-se que, nos termos do art.º 18.º n.º 2 da Lei do Cibercrime, se no decurso da ação encoberta se efetuar a utilização de meios e dispositivos informáticos, ter-se-á que observar o regime previsto para a interceção das comunicações.

2. A IMPORTÂNCIA DA CIÊNCIA FORENSE DIGITAL

2.1. A ORIGEM DA CIÊNCIA FORENSE DIGITAL E A SUA EVOLUÇÃO

No capítulo anterior, procurou-se analisar os meios de obtenção de prova, previstos no âmbito da Lei do Cibercrime, com especial enfoque na pesquisa de dados informáticos e sempre na perspetiva de delimitar corretamente o seu âmbito de aplicação. Conforme se referiu, a prova digital assume um caráter transversal de acordo com o disposto no art.º 11.º da Lei do Cibercrime.

A título de exemplo, dir-se-á ainda que, atendendo ao facto da haver cada vez mais utilizadores de dispositivos eletrónicos, sejam eles computadores ou *smartphones,* poderá ser determinante numa investigação de um crime de homicídio, a análise do *smartphone* do suspeito, podendo aí serem localizadas, por exemplo, pesquisas na internet que venham a esclarecer o *modus operandi* utilizado pelo autor. De igual modo, ao investigar o crime de tráfico de droga ou terrorismo, poderão ser encontradas conversações em plataformas de comunicação instantâneas que permitam a identificação de outros suspeitos. Também na investigação da criminalidade económica-financeira, a análise forense ao computador do suspeito poderá permitir a identificação, por exemplo, de contas bancárias onde as quantias monetárias obtidas ilicitamente foram creditadas e, por conseguinte, a sua apreensão.

Para que seja possível proceder à recolha de todo este acervo de prova digital é essencial haver investigadores especializados em Ciência Forense Digital.

A Ciência Forense, segundo a Academia Americana de Ciências Forenses, é a aplicação de princípios científicos e práticas tecnológicas, ao estudo de soluções, designadamente para questões criminais ou civis, tendo em vista os fins da justiça[49].

[49] Esta definição terá sido apresentada pelo Conselho da Academia Americana de Ciências Forenses em 1993 (https://aafs.org/AAFS/About-Us/History.aspx).

Segundo John R. Vacca, a Ciência Forense Digital consiste no ramo da Ciência Forense que visa a "recolha, preservação, análise e apresentação da prova digital" (Vacca, 2005, p. 4).

Trata-se assim de um ramo especializado que visa assegurar a cadeia da custódia da prova, sendo este conceito definido da seguinte forma:

> Uma técnica jurídico-científica processual que tem como fundamento (e pressuposto), fim e limite conservar a identidade (originalidade) e autenticidade (integridade) da prova recolhida, apreendida com a realização de um meio de obtenção de prova constitucional e legalmente admissível (…), de modo a ser submetida, nos casos determinados por lei ou despacho judicial, a meio de prova – perícia técnico científica – por funcionário ou pessoa habilitada legal, técnica e cientificamente (Valente, 2020, p. 93).

É comum apontar-se a génese da Ciência Forense Digital no ano de 1984, aquando da criação do CART – *Computer Analysis and Response Team* por parte do FBI. Este organismo foi criado com o propósito de satisfazer as várias solicitações judiciais de perícias informáticas (Rodrigues, 2011).

Com o passar do tempo, o aumento de pedidos de perícias informáticas ditou que as funções e o modo de organização do CART fossem replicados noutras agências de combate à criminalidade nos E.U.A e também em países da Europa.

A preocupação inicial da Ciência Forense Digital prendia-se com o modo de analisar a prova digital, tendo-se vindo a concluir que esta análise teria que ser realizada em "ambiente laboratorial fortemente controlado e com um rígido controlo da cadeia de produção e análise das provas (*Chain of custody*)" (Rodrigues, 2011, p. 482).

Neste seguimento, nos anos 90, os *Technical Working Groups* viriam a ser substituídos pelos *Scientific Working Group*, tendo-se vindo a estabelecer os primeiros *standards* para exame da prova digital pela IOCE – *International Organization on Computer Evidence*.

Em 1998 foi criado o SWGDE – *Scientific Group On Digital Evidence.* Passado um ano este grupo de trabalho, conjuntamente com o IOCE apresentou na *International Hi-Tech Crime and Forensics Conference*, realizada em Londres, que decorreu entre 4 a 7 de outubro, um documento onde se defende a adoção de padrões para a troca de prova digital, entre os vários países, bem como a necessidade de se aprofundar a reflexão e debate sobre esta temática[50].

A constante evolução tecnológica tem trazido uma miríade de dispositivos eletrónicos suscetíveis de conter elementos de prova.

Deste modo, a Ciência Forense Digital, num esforço da adaptação às novas realidades veio a criar ramos do conhecimento mais especializados, tais como as Ciências Forenses de Redes (*network forensics*), de dispositivos móveis (*mobile device forensics*) ou de *malware* (*malware forensics*) (Ramalho, 2017).

As mais recentes publicações do SWGDE de diversos manuais de boas práticas nos domínios da recolha e análise de prova em computadores, em telemóveis, dispositivos GPS portáteis, bem como em *cloud,* entre outros, constituem um bom exemplo da tentativa de acompanhamento da evolução da tecnologia[51].

Na Europa, salienta-se o papel do ECTEG (*European Cybercrime Training and Education Group*), organismo entretanto fundado pela Comissão Europeia, em colaboração estreita com a EUROPOL e a CEPOL, cuja missão é apoiar as polícias e magistrados dos Estados membros da União Europeia na luta contra o cibercrime.

Este organismo visa, através da formação, melhorar e uniformizar as capacidades técnicas e científicas dos profissionais destas áreas em parceria com especialistas das polícias, do mundo académico e do setor privado, oferecendo diversos cursos de especialização, designadamente em sistema operativo Linux, Mac OS, *dark web* e moeda virtual, destacando-se por fim o

[50] Mais informação sobre a origem do SWGDE está disponibilizada em https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm (Consultada a 03/04/2020).

[51] Estes documentos podem ser acedidos em https://www.swgde.org/documents/published (Consultado a 03/04/2020).

projeto *e-First*, no qual a Polícia Judiciária é um membro cofundador e que constitui uma plataforma de autoformação, disponível 24/7, em 17 idiomas[52] para *first responders*[53].

Este curso permite que os polícias que atuam em primeira linha auxiliem vítimas de crimes relacionados com as novas tecnologias de forma a, por exemplo, instruir corretamente a queixa-crime, bem como identificar e apreender elementos suscetíveis de servirem de prova.

Os cursos que vêm sendo organizados assumem a preocupação da necessidade de permanente atualização, não descurando a importância em uniformizar procedimentos.

Paralelamente são criadas unidades especializadas para a recolha, análise e perícias informáticas nas instituições vocacionadas para a investigação criminal, salientando-se que, em Portugal, nos termos do art.º 43.º do DL n.º 137/2019, de 13 de setembro (Nova estrutura organizacional da Polícia Judiciária), estas competências estão atribuídas à Unidade de Perícia Tecnológica Informática.

No que tange à investigação do cibercrime, nos termos do art.º 33.º deste diploma, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica é a unidade competente, evidenciando-se que, no âmbito desta, funciona uma equipa de investigação digital que goza de autonomia técnica e científica e tem como função, designadamente dar apoio em ações de caráter técnico para recolha de prova digital, nomeadamente ações encobertas e interceções de dados (n.º 4, al. f)), bem como apoiar investigações que exijam conhecimentos técnicos especializados relativos, nomeadamente a redes de anonimização, mercados e moedas virtuais, análise de programas maliciosos (n.º 4, al. g)).

[52] À data de maio de 2019: https://www.ecteg.eu/running/first-responders/ (Acedido a 03/04/2020).
[53] Estes cursos podem ser consultados em: https://www.ecteg.eu/course-packages/ (Acedido a 03/04/2020).

2.2. PRINCÍPIOS ATINENTES À PROVA DIGITAL

Na sequência do que vem sendo exposto, no âmbito, nomeadamente, dos cursos ministrados têm vindo a ser enunciados princípios atinentes à prova digital, salientando-se, pela sua relevância, a sistematização internacional da *Association of Chief Police Officers*[54] e que, entre os autores portugueses, encontra acolhimento na apresentação de Benjamim Silva Rodrigues que elenca deste modo, os princípios da não alteração da prova eletrónico-digital no ato de recolha; da especialização ou qualificação do pessoal de investigação forense digital; da documentação de todas as fases de acesso, recolha, armazenamento, transferência, preservação, ou apresentação/repetição da prova eletrónico-digital; da pessoalidade do controlo da cadeia da custódia da produção da prova digital e da responsabilização repartida dos vários intervenientes na produção da prova eletrónico-digital no respeito dos princípios forenses digitais (Rodrigues, 2011, pp. 45-46).

A especificidade da prova digital exige ainda, segundo Blakeslee (citado por Antunes & Rodrigues, 2018), que a prova deve ser legalmente admissível quanto à sua forma de obtenção e tecnicamente incontestável. Esta característica implica que a origem da prova seja verificável e a "integridade tem que ser demonstrável através dos seguintes meios: por certificação, através de um resumo digital; por duplo controlo, nomeadamente notas e apontamentos, ou por verificação técnica e humana" (Antunes & Rodrigues, 2018, p. 138).

2.3. AS ETAPAS DO PROCEDIMENTO FORENSE

Referenciados os princípios que devem nortear a recolha de tratamento da prova digital, far-se-á uma breve referência, de seguida, às etapas do procedimento forense.

[54] https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. (Consultado em 03/04/2020. *Vide* p. 6).

Foi entre 7 e 8 de agosto de 2001, em Nova Iorque, aquando da primeira reunião promovida pelo *Digital Forensics Research*, que surgiu o primeiro modelo de Ciência Forense Digital (Rodrigues, 2011).

Esta reunião constitui um marco histórico de grande importância, dado que promoveu a reflexão e discussão "entre a comunidade académica e a comunidade tecnológica (laboratórios forenses, administradores de sistemas informáticos, entre outros), com vista à definição do campo e identificar as dificuldades e desafios emergentes nesta matéria" (*Idem*, p. 485).

O modelo derivado desta reunião assentava em sete etapas distintas: 1) Identificação; 2) Preservação; 3) Recolha; 4) Exame; 5) Análise; 6) Apresentação; 7) Decisão.

Desde essa data, surgiram vários modelos. No entanto, sendo certo que não existe um consenso sobre o método a aplicar no processo de recolha, preservação e apresentação de prova digital, também é verdade que no âmbito dos vários modelos existentes, cada um com as suas etapas e procedimentos específicos, é possível encontrar um padrão comum de atuação marcado pelo rigor científico (Ramalho, 2017).

Deste modo, acompanhando Silva Ramalho, apresenta-se como referência o procedimento forense proposto pelo NIST (*National Institute of Standards and Technology*).

Este procedimento forense reconduz-se a quatro fases fundamentais: 1) recolha; 2) exame; 3) análise; 4) apresentação do relatório (Jansen, Ayers, & Brothers, 2014, pp. 3-1).

A primeira etapa, não obstante, ser designada por recolha, implica, *a priori*, a identificação das eventuais fontes de prova digital, que poderá ser um computador portátil, um smartphone, dispositivos de armazenamento USB, podendo ainda estar armazenada na *cloud*. Será a partir desta possível identificação que será escolhida uma determinada abordagem e os recursos adequados. A este respeito cumpre evidenciar que há autores que costumam fazer referência a uma fase prévia e autónoma de preparação, segundo a qual o perito, após ter uma noção do suporte onde poderá ser encontrada a prova digital, deverá eleger a abordagem mais adequada à sua preservação. (Antunes

& Rodrigues, 2018, pp. 140-141)[55]. Obviamente que a preparação constituiu um momento bastante importante, no entanto, entende-se não ser necessário proceder à sua autonomização, em termos teóricos.

É também no âmbito desta fase que se procede à etiquetagem e registo de toda a informação relevante encontrada num determinado cenário. Deste modo, constitui uma boa prática fotografar e gravar em vídeo os sistemas informáticos visados, de modo a perceber a sua exata localização, o seu estado de funcionamento, e todas as ligações existentes, devendo ainda anotar-se os dados dos dispositivos: marca, modelo, número de série, as informações prestadas pelos utilizadores e as credenciais de acesso a esses equipamentos (Ramalho, 2017).

Ao abordar os sistemas informáticos, designadamente computadores, é comum distinguir dois cenários: *dead or powered off machines* e *live or running machine* (Sammons, 2014). Na primeira situação, estando o sistema informático desligado é consensual apreender-se o equipamento, etiquetar o mesmo e transportar para o laboratório a fim de ser, posteriormente, examinado (Cybercrime Division, 2014).

Dias Ramos adverte ainda que ao proceder-se à ligação do equipamento poderão perder-se elementos com interesse para a investigação, tais como a última vez que o sistema foi desligado, os últimos documentos que foram acedidos, entre outros (Ramos, 2014).

No segundo cenário, estando o computador ligado defendia-se que se deveria desligar o mesmo diretamente na fonte de energia elétrica (Sammons, 2014, p. 54).

Atualmente é incontestável a importância de abordar o sistema informático que se encontra ligado – *live forensics*, alertando-se para a necessidade de fotografar, filmar e registar toda a informação pertinente relativamente ao mesmo, salientando-se a possibilidade de preservar dados que pela sua natureza volátil serão irrecuperáveis caso se desligue o sistema

[55] Neste sentido também Benjamim Silva Rodrigues, cujo modelo, por si defendido, designado por Dinâmico-Reversivo é estruturado em oito fases salientando-se que a primeira fase é a da obtenção da respetiva autorização judicial e de preparação estratégica de abordagem à prova eletrónico-digital (Rodrigues, 2011, pp. 500-501).

informático da fonte de alimentação. De entre esses dados salienta-se a memória RAM (*Random Access Memory*). A memória RAM pode conter muita informação relevante, destacando-se os processos em curso, utilizadores com sessão iniciada, *passwords e* informação sem estar encriptada. Com efeito, se o sistema informático tiver configurado um programa de encriptação, caso o mesmo seja desligado, a informação ficará novamente protegida pela encriptação. Outra das desvantagens de desligar de forma repentina o sistema informático é o risco de danificar os dados (Sammons, 2014, p. 57).

Evidenciadas as vantagens do *live forensics,* refira-se ainda que para recolher a informação guardada em RAM – *memory dump,* também existe *software* forense específico, que deverá ser utilizado através de dispositivos amovíveis, tais como *pens USB*, de modo a recolher a informação apenas para o dispositivo e não para o computador que está a ser examinado (Ramalho, 2017).

Após se ter abordado as vantagens de recolher os dados voláteis, salientando-se que atendendo à sua natureza se deverá dar prioridade aos mesmos, cuidar-se-á agora da recolha dos restantes dados, com vista à sua preservação.

Para esse efeito é necessário realizar um "conjunto de ações destinadas a manter o estado da prova, tal como foi encontrada e onde foi encontrada, com o intuito de permitir uma recolha integral e certificada (aquisição e validação)" (Antunes & Rodrigues, 2018, p. 145). A práxis forense com vista a garantir a autenticidade, integridade e disponibilidade da totalidade desses dados consiste na realização de uma clonagem ou cópia de imagem através de "um processo de duplicação exata do disco, *bit* por *bit*, incluído espaço livre, ficheiros eliminados e *metadata*" (Ramalho, 2017, p. 123).

O processo, quando aplicado ao disco rígido de um computador, é realizado com recurso a programas informáticos forenses ou de *hardware* criados *ad hoc,* muitos deles já incluindo a necessária funcionalidade de bloqueio da escrita, que impossibilita a alteração da prova.

A título exemplificativo, indica-se o programa de informática forense FTK Imager[56], bem como a recente solução de *hardware Tableau TX1 Forensic Imager.*[57]

No que concerne aos smartphones cumpre referir a existência dos dispositivos tipo UFED (*Universal Forensic Extraction Device*), comercializados pela empresa Cellebrite, comummente utilizados pelas Polícias que permitem extrair o conteúdo integral desses equipamentos e posteriormente a análise dessa informação[58].

Outro procedimento fundamental que atesta a autenticidade e integridade da prova recolhida diz respeito à validação da prova antes e posteriormente à sua recolha. Para que isso seja possível é necessário "calcular a soma binária, ou resumo digital, tanto da base física do suporte de dados que é a prova, como das cópias forenses que sejam realizadas. O resumo digital de ambas deverá ser igual" (Antunes & Rodrigues, 2018, p. 159). Este resumo digital resulta da aplicação da já referida função *hash*, "que utiliza um algoritmo que calcula a soma binária dos dados apresentados à função, retornando uma sequência de bits de comprimento fixo em numeração hexadeximal" (*Ibidem*). Estes valores são conhecidos poder códigos *hash.*

Os algoritmos mais utilizados para obter o resumo digital são o MD5 (*Message-Digest Algorithm 5*) e o SHA-1 (*Secure Hash Algorithm*).

Realça-se o facto de praticamente todos os programas de informática forense e das soluções de *hardware* criadas *ad hoc* permitirem gerar o resumo digital nos moldes que foram expostos (*Idem*).

Esta forma de validação, conforme se referiu, aquando da análise do regime legal da apreensão dos dados informáticos, encontra-se prevista no art.º 16.º, n.º 8 da Lei do Cibercrime, sob a designação de "assinatura digital".

Como bem elucida Silva Ramalho, a exigência técnica de realizar uma cópia integral de um determinado sistema informático, de modo a acautelar a

[56] Para mais informações sobre o FTK Imager: https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager (Consultado a 03/04/2020).
[57] Sobre esta solução poderá consultar-se o *site*: https://www.guidancesoftware.com/tableau (Acedido a 03/04/2020).
[58] Mais informação sobre o UFED poderá ser obtida em: https://www.cellebrite.com/en/ufed/ (Acedido a 03/04/2020).

disponibilidade, autenticidade e integridade dos dados, tem de se coadunar com o princípio da proporcionalidade que deverá sempre ser observado no âmbito das diligências de recolha de prova. Assim, não obstante o investigador ficar na posse de um volume elevado de informação, que em muitos casos extravasará o objeto da investigação, este deverá sempre nortear-se, nas pesquisas a realizar, pelos factos concretos em investigação (Ramalho, 2017).

Na segunda fase, a de exame, destaca-se a necessidade de filtrar os dados de um determinado sistema informático, visando-se assim apenas a recolha da prova digital relevante para uma determinada investigação criminal.

Trata-se de uma fase, tendencialmente, morosa, mas fundamental para evitar a clonagem desnecessária do conteúdo de todos os sistemas informáticos na posse de um suspeito ou da apreensão massiva desses equipamentos. Basta imaginarmos a realização de uma busca a uma empresa com dezenas de computadores, a uma instituição bancária ou a um estabelecimento de saúde para se perceber facilmente a importância de procurar primeiro localizar a prova pertinente através de uma triagem forense e, caso a mesma seja localizada, proceder à sua recolha a partir da fonte efetivamente relevante.

Este exame consistirá numa triagem forense que permitirá ainda em muitas situações confrontar, desde logo, o suspeito com os elementos de prova no âmbito de um interrogatório, podendo ainda os mesmos ser relevantes para aplicação de uma determinada medida de coação.

Para tal, o examinador também recorrerá a ferramentas de triagem forense que garantam a integridade da prova e que permitam realizar pesquisas por palavras-chave (Ramos, 2014), ou por determinado tipo de ficheiros, por exemplo de imagem, sendo este tipo de pesquisa muito usual na investigação do crime de pornografia de menores.

A título de exemplo destaca-se a ferramenta de triagem forense DEI – *Digital Evidence Investigator - Triage Investigator*, comercializada pela empresa ADF Solutions[59].

[59] Sobre o *Triage Investigator:* https://www.adfsolutions.com/triage-investigator (Acedido a 03/04/2020).

Tendo sido realizada a triagem forense e a recolha dos dados informáticos suscetíveis de serem relevantes para uma determinada investigação criminal, importará acondicionar corretamente os suportes dessa prova e transportá-los tendo em atenção que os dispositivos eletrónicos "são sensíveis à temperatura, à humidade, a choques, à eletricidade estática, a campos magnéticos" (Antunes & Rodrigues, 2018, p. 149). Deste modo, deve-se usar material antiestático e não plástico, devendo ainda as embalagens, onde o material é transportado, serem corretamente etiquetadas (*Ibidem*).

A análise será realizada sobre os dados duplicados durante a fase de aquisição. Esta fase consiste num trabalho minucioso onde se visa também, designadamente, recuperar dados que tenham sido apagados e que se afigurem relevantes para a prova, bem como a correlação de todos os elementos apurados.

Trata-se assim de uma fase laboratorial, sendo necessários peritos devidamente credenciados, bem como estações forenses e aplicações informáticas adequadas, salientando-se o *Encase*[60]*, NUIX*[61]*,* Intella[62], *Magnet Axiom*[63] bem como a solução gratuita *Autopsy*[64] (Antunes & Rodrigues, 2018).

A última fase do modelo de Ciência Forense Digital adotado consiste na fase de apresentação. Nesta fase será elaborado um relatório onde conste a identificação do objeto de exame, os métodos utilizados desde a recolha da prova até à análise dos dados e as conclusões que nessa sequência foram obtidas (*Ibidem*).

Evidencia-se a importância do relatório ser elaborado numa linguagem compreensível a todos os intervenientes processuais, adotando-se, se necessário, um glossário de termos, bem como um índice para se localizar rapidamente a informação relevante.

---

[60] Sobre o *Encase* poderá consultar-se: https://www.guidancesoftware.com/encase-forensic (Acedido a 03/04/2020).
[61] Sobre o NUIX poderá consultar-se: https://www.nuix.com/solutions/investigations (Acedido a 03/04/2020).
[62] Sobre as potencialidades do *Intella*: https://www.vound-software.com/solutions (Acedido a 03/04/2020).
[63] Sobre o *Magnet Axiom*: https://www.magnetforensics.com/products/magnet-axiom/ (Acedido a 03/04/2020).
[64] Sobre o *Autopsy*: https://www.autopsy.com/ (Acedido a 03/04/2020).

Atualmente é habitual, na prática forense, entregar-se um relatório impresso e um em formato HTML. “A capacidade de usar hiperligações e marcadores para direcionar o leitor para um local específico ou exibir um determinado item, tem um impacto muito positivo na leitura dos relatórios (…) Recomenda-se sempre que possível o recurso a uma solução híbrida que contemple os dois métodos e permita a análise inequívoca de toda a informação disponível sobre a análise digital efetuada” (Antunes & Rodrigues, 2018, p. 185).

As ferramentas forenses utilizadas para a análise dos dados são cada vez mais completas e intuitivas, permitindo elaborar relatórios de forma célere e com recursos importantes na demonstração da prova, tais como esquemas de correlação e organização de dados, podendo os mesmos serem visualizados, designadamente por linha do tempo.

Relativamente ao modo de entrega do relatório, estas ferramentas permitem que o mesmo seja elaborado em vários formatos (*Excel, Word*, PDF, HTML).

Percorridas as fases fundamentais do modelo de Ciência Forense Digital adotado, procurar-se-á abordar de seguida as principais técnicas anti-forenses que vêm sendo utilizadas e que constituem um obstáculo à recolha de prova de digital.

2.4. AS PRINCIPAIS TÉCNICAS ANTI-FORENSES

Conforme vem sendo referido, a Ciência Forense Digital tem registado um avanço notável nos últimos trinta anos, num esforço de adaptação à realidade tecnológica que se encontra em constante mutação.

Estas mudanças tecnológicas têm sido aproveitadas na prática de diversos crimes dificultando ainda a ação das autoridades na recolha e análise de elementos suscetíveis de servir de prova.

Numa definição avançada por John Barbara as técnicas anti-forenses visam eliminar, adulterar ou dissimular determinado tipo de dados de forma a obviar a recolha desses elementos que poderiam servir de prova (citado em Sammons, 2014).

A eliminação de dados enquanto técnica anti-forense não se deve confundir com o simples apagar de ficheiros. Com efeito, quando se apaga um ficheiro, isto não significa que ele seja eliminado definitivamente. Apenas se remove o apontador a esse ficheiro, sendo a localização no respetivo disco rígido marcada como espaço não alocado, tornando-a disponível para novos dados que venham a ser armazenados. Deste modo é possível, com as ferramentas forenses adequadas, recuperar esses dados (Santos, Bessa, & Pimentel, 2008).

Destaca-se também a probabilidade de existirem elementos com interesse para uma investigação criminal nos ficheiros temporários da internet ou no histórico de endereços visitados (*Ibidem*).

A eliminação de dados, enquanto técnica anti-forense visa deste modo "tornar irrecuperáveis os ficheiros eliminados de um sistema informático através da sua substituição por uns, zeros ou caracteres aleatórios, muitas vezes de forma repetida" (Ramalho, p. 166). Para tal são utilizados programas, tais como o ERASER e o CCleaner.

A adulteração de dados consiste noutro conjunto de técnicas que visam pôr em causa o princípio da não alteração da prova eletrónico-digital no ato de recolha.

Silva Ramalho refere como exemplos a alteração dos metadados de certos ficheiros e a modificação de extensões e assinaturas de documentos informáticos (Ramalho, 2017).

O conceito de metadados "designa o conjunto de informações sobre um determinado ficheiro" (Antunes & Rodrigues, 2018, p. 169). Os metadados poderão revelar muitas informações com interesse para uma determinada investigação, designadamente a identificação do autor, datas e horas (*Ibidem*). Por exemplo uma fotografia digital armazena este tipo de informação num ficheiro EXIF (*Exchangeable Image File Format*), onde poderá apurar-se a data e hora a que a foto foi tirada, qual a câmara utilizada e, eventualmente, informação acerca da localização exata onde foram tiradas (Cybercrime Division, 2014).

Assim, os programas anti-forenses ao alterar por exemplo a data da criação de um ficheiro, poderão dificultar a sua deteção aquando da realização

da triagem forense[65]. O mesmo sucede quando se procede à modificação de extensões. Basta imaginar um cenário de crime, no qual um suspeito de pornografia infantil altera, previamente à diligência policial, as extenções de ficheiros de imagem e de vídeo ilícitos para a extensão de ficheiro executável, para se perceber a dificuldade no âmbito da recolha de prova digital (Ramalho, 2017).

No âmbito da dissimulação de dados ir-se-á abordar os *softwares* de anonimização, a esteganografia e a encriptação.

Para compreender a anonimização ter-se-á que fazer referência ao conceito de *Deep Web* e à forma como se pode aceder aos conteúdos existentes na mesma. É comum recorrer-se a imagem de um iceberg para definir a internet. A parte visível constitui a internet como a conhecemos, com a informação indexada, sendo a parte imersa a *Deep Web*, que não é acessível através dos motores de busca utilizados habitualmente (*Google Chrome, Microsoft Edge, Mozilla Firefox*, etc) (Ramos, 2015, p. 121).

Para perceber a importância da *Deep Web*, refira-se que se estima que esta represente 96% da dimensão da internet, no que diz respeito ao volume de conteúdos disponibilizados (Antunes & Rodrigues, 2018).

Na *Deep Web*, podem-se encontrar diversos conteúdos, podendo existir conteúdos ilegais. Nestes casos é comum falar-se em *Dark Web.* O acesso à *Deep Web* realiza-se através de *softwares* específicos. Os mais conhecidos são o *The Onion Router*, abreviadamente TOR e o *Freenet*. Ambos visam a anonimização dos seus utilizadores e dos conteúdos acedidos por estes, sendo que o *Freenet* utiliza tecnologia P2P (*peer-to-peer*), ou seja, através de nódulos criados entre vários utilizadores.

No caso do TOR, o mesmo utiliza um sistema encriptado por camadas, semelhante a uma cebola (*onion*). Desta forma os utilizadores não se ligam diretamente ao servidor/página que pretendem uma vez que a rede TOR vai criar conexões, através da internet, com diversos computadores existentes na sua

[65] Silva Ramalho destaca o programa Timestomp para alteração de metadados (Ramalho, 2017).

rede. Estas conexões cifradas são apagadas à medida que a informação circula na rede, impedindo desta forma a identificação originária (Ramos, 2015, p. 121).

A esteganografia consiste, em termos informáticos, em ocultar determinada informação noutros ficheiros eletrónicos (Santos, Bessa, & Pimentel, 2008), existindo vários programas para esse efeito. Deste modo, a análise a ser realizada deverá aferir desde logo a existência de *software* existente no computador suspeito que possibilite a ocultação de informação, devendo ainda proceder-se à análise dos ficheiros, procurando propriedades incomuns (Cybercrime Division, 2014).

A encriptação ou cifragem é "um processo de transformar informações (texto simples), através de um algoritmo criptográfico (cifra), tornando-o ilegível (texto cifrado) para qualquer pessoa, exceto para aqueles que possuem a chave" (Antunes & Rodrigues, 2018, p. 172).

A encriptação tem vindo a ser generalizada e disponibilizada a título gratuito como garantia da privacidade. Nos computadores são várias as aplicações que possibilitam a encriptação, referindo-se a título de exemplo as soluções de encriptação do disco rígido *Windows Bitlocker* ou o *Veracrypt.* Também nos *smartphones*, bem como em diversas plataformas, comummente utilizadas vieram a ser adotadas valências de encriptação pelas empresas responsáveis. É o caso, por exemplo, da *Apple, Google, Samsung* (Fernandes, 2018, p. 63).

No que concerne às aplicações para comunicação instantânea, estas também têm vindo a adotar a encriptação ponto a ponto, o que as torna inacessíveis às autoridades, é o caso da conhecida aplicação *Whatsapp* (Lewis, Zheng, & Carter, 2017).

O relatório da Europol IOCTA 2019 tem sublinhado as dificuldades que a encriptação trouxe, quer ao nível da proteção da informação, quer das comunicações constituindo um dos maiores desafios para a Ciência Forense Digital.

Recorde-se que já em 2010 Garfinkel referia que a "idade de ouro" da Ciência Forense Digital, que teria ocorrido entre 1999 e 2007, tinha chegado ao fim, antevendo-se uma crise devido a diversos fatores, entre os quais o facto da

encriptação inviabilizar o acesso aos dados, as dificuldades de enquadrar as etapas do modelo forense na recolha e preservação da prova digital armazenada na *cloud*, bem como a grande diversidade de dispositivos para analisar e de sistemas operativos (Garfinkel, 2010).

2.5. DA NECESSIDADE DE UTILIZAÇÃO DE MEIOS OCULTOS AO VISADO

Do que se expôs anteriormente constatam-se, nos dias de hoje, várias dificuldades, no concerne à obtenção de prova digital. Como se referiu uma das dificuldades mais prementes é a encriptação.

As opções dos Estados face à encriptação podem reconduzir-se a três: o *laissez faire*, ou seja, as empresas podem comercializar qualquer tipo de solução que permita a encriptação. Esta opção poderá ter um impacto significativo nas investigações criminais levadas a cabo pelas autoridades. Outra opção é de adotar restrições à produção e aquisição de soluções que permitam a encriptação. No âmbito destas medidas também se poderá determinar que os Fornecedores de Serviços de Internet procedam ao bloqueio de produtos que permitam a encriptação. Esta medida poderá não ter o impacto esperado dado que poderá levar as empresas a apostar noutras soluções, designadamente a não retenção de quaisquer dados do cliente. A terceira opção consiste na possibilidade das autoridades explorarem as vulnerabilidades do sistema informático encriptado alvo de modo a instalar *software* que permita a obtenção desses dados ou a sua monitorização (Lewis, Zheng, & Carter, 2017, pp. 26-27).

Em Portugal, Silva Ramalho refere-se, a propósito desta solução, à utilização de *malware,* como sendo a expressão mais adequada, dado que se trata de um meio "intrusivo, insidioso e, portanto, malicioso em relação ao sistema no qual se instala" (Ramalho, 2013, p. 201). Recentemente, Duarte Rodrigues Nunes referiu-se a esta solução como *benware*, visto que está em causa a utilização, por parte das autoridades, de programas informáticos para fins de prevenção ou repressão criminais (Nunes D. R., 2020).

Assim sendo, o *benware* consubstancia um recurso tecnológico apto a, de forma eficaz, por exemplo, concretizar uma pesquisa remota, sem o conhecimento do visado, assim como a realizar uma interceção de dados.

Estes programas informáticos poderão ser instalados de várias formas, designadamente pelo próprio visado, sem este saber, através do *download* de um anexo constante de uma mensagem de correio eletrónico, via suporte físico removível (uma *pendrive* por exemplo) ou através da infeção via *web browser* (Ramalho, 2013).

No que concerne às potencialidades destes programas informáticos, evidencia-se a sua grande abrangência pois é possível não só copiar a informação de um determinado sistema informático, num único ato, mas também e de forma contínua monitorizar esse sistema informático, sendo ainda possível ativar os microfones, a *webcam*, registar a utilização do teclado, e outras até à presente data desconhecidas (Batista, 2018).

Colocando o enfoque nas vantagens na utilização destes meios, salienta-se a possibilidade de superar os obstáculos de programas destinados à encriptação de dados cada vez mais generalizados, monitorizar a navegação na internet, permitir, através de *keyloggers*, a obtenção de *passwords*, a obtenção de dados que poderão vir a ser eliminados e o acesso a dados na *cloud*, que, de outra forma, seriam mais difíceis de obter (Nunes D. A., 2019, pp. 813-817).

A utilização destes meios, no âmbito da investigação criminal, terá ocorrido primeiramente nos E.U.A (Ramalho, 2013). Apresentar-se-á, de forma sucinta, uma breve resenha histórica da utilização destes meios, nesse país, com vista a perceber a sua evolução.

O primeiro caso que tem vindo a ser apontado, reporta-se ao uso por parte do FBI, em 1999, de um *keylogger*, ou seja de um "*software* que grava e envia informação acerca das teclas premidas pelo utilizador de um sistema informático" (*Idem*, p. 203).

Esta utilização ocorreu no âmbito de uma investigação a Nicodemo Scarfo, um membro de uma organização mafiosa suspeito da prática de vários ilícitos criminais relacionados com a gestão de um negócio de jogo ilegal, que teria armazenado no seu computador ficheiros encriptados que se suspeitava

serem relevantes para a investigação. Este *keylogger* veio a ser instalado fisicamente. Passados catorze dias tinha sido possível obter a palavra-passe do programa de encriptação, PGP (*Pretty Good Privacy*) e, consequentemente, o acesso ao conteúdo desses ficheiros (Quinlan & Wilson, 2016).

A forma de instalação destes programas veio a evoluir, passando a realizar-se de forma remota, ultrapassando assim as dificuldades práticas do acesso físico aos computadores dos suspeitos da prática de crimes e constituindo uma resposta mais eficaz à criminalidade transnacional (Ramalho, 2013).

Deste modo, em 2001, surgiu o *Magic Lantern,* um *keylogger*, que podia ser instalado remotamente no sistema informático alvo, involuntariamente pelo próprio suspeito, através da abertura de anexos constantes de mensagens de correio eletrónico e através da exploração de vulnerabilidades no sistema operativo instalado no sistema informático alvo (*Idem*, p. 214).

No ano de 2007 veio a ser divulgado pela Comunicação Social a utilização de um programa designado por CIPAV (*Computer and Protocol Address Verifier*), no âmbito da investigação, que visava identificar o autor de várias ameaças de bomba. Este programa, segundo informação disponibilizada recolhia também o endereço IP, o MAC (*Media Access Control*), informação do sistema operativo, qual o *browser* de internet utilizado, o nome do computador e histórico de internet, bem como as comunicações. Este programa permitiu localizar, identificar e deter um jovem estudante de 15 anos (Quinlan & Wilson, 2016, p. 4).

Em março de 2013, o FBI solicitou uma autorização judicial para a instalação de um programa informático com vista a identificar um desconhecido, que acedeu ilicitamente à conta de correio eletrónico de uma vítima e, após criar uma conta semelhante, tentou transferir dinheiro da conta bancária desta. Não obstante esta autorização vir a ser recusada e do relatório do FBI não constar como o programa seria instalado, importa referir que esse relatório especificava que o programa recolhia o IP, histórico de internet, nome dos utilizadores e *password*s, documentos, registos de *chat* e de correspondência, quando o

computador estava a ser usado, quais as aplicações utilizadas, localização do sistema informático e tirava fotografias através da câmara (*Idem*, p. 5).

Outro dos marcos históricos na utilização destes meios, diz respeito à investigação do *site Playpen,* onde era possível obter conteúdos dedicados à pornografia infantil. Em 2015, o FBI recorreu à NIT (*Network Investigative Technique*) como forma de ultrapassar a anonimização propiciada pelo *Tor Browser*. Assim, procedendo à infeção de fóruns do *site Playpen,* entre 20 de fevereiro e 4 de março, foi possível obter a localização, bem como outras informações que permitiram a identificação de cerca 1300 computadores que se ligavam a esses fóruns (*Idem*, p. 7). Esta investigação terá durado mais de dois anos, tendo culminado na identificação de 300 vítimas e na detenção de mais de 800 pessoas [66].

No dia 2 de dezembro de 2015, o casal Syed Rizwan Farook e Tashfeen Malik, em São Bernardino, lançaram um ataque com armas de fogo, tendo matado catorze pessoas. Estes indivíduos destruíram os seus telemóveis e computadores, apenas tendo ficado um IPHONE 5C, que seria um telemóvel de trabalho de Farook. Esse telemóvel estava protegido com encriptação.

Em fevereiro de 2016, o FBI conseguiu uma ordem judicial para que a APPLE auxiliasse a aceder ao conteúdo desse telemóvel, sendo certo que isso implicaria a criação de uma *backdoor*. Isto causou um grande debate no meio académico e técnico, tendo as principais empresas tecnológicas: Google, Facebook, Twitter, Yahoo e Ebay se posicionado ao lado da APPLE no sentido de que não seria adequado criar *backdoors* que inevitavelmente comprometeriam a segurança dos produtos que estas comercializavam. Não obstante este debate, o que é certo é que o FBI veio a aceder ao conteúdo desse telemóvel, desconhecendo-se pormenores acerca deste acesso (Quinlan & Wilson, 2016).

No corrente ano, merece destaque a recente operação conjunta de várias policias europeias, que permitiu, através de *malware,* aceder à plataforma de

[66] *Vide*: https://www.cmjornal.pt/mundo/detalhe/900-detidos-em-investigacao-do-fbi-e-europol-sobre-porngrafia-infantil (Consultada a 20/09/2020).

comunicação encriptada que estava a ser utilizada por milhares de criminosos: Encrochat e, assim, deter centenas de indivíduos[67].

Esta breve resenha histórica demonstra a enorme evolução e importância destes meios informáticos para obtenção de elementos suscetíveis de servir de prova, no contexto da investigação criminal, no período compreendido entre 1999 e a presente data.

No que concerne ao enquadramento legal para a utilização de *malware* no âmbito das investigações criminais, constata-se que as autoridades norte-americanas têm solicitado a respetiva autorização nos termos do art.º 41.º do *Federal Rules of Criminal Procedure*, que diz respeito ao regime aplicável às buscas e apreensões, salientando-se que a alteração a este artigo, ocorrida em dezembro de 2016, veio permitir a emissão de mandados, quando a localização do sistema informático for desconhecida, designadamente por ter sido ocultada por meios tecnológicos[68](Directorate General For Internal Policies, 2017). A instalação de *malware* será, assim, enquadrável no conceito de busca (*remote computer searches*) e, num segundo momento, a extração da informação relevante e consequentemente a obtenção da mesma por via remota ao conceito de apreensão (Ramalho, 2017). A referida norma não densifica de forma exaustiva em que termos esta utilização poderá ser efetuada, sendo ainda necessário ter presente o disposto na Quarta Emenda à Constituição norte-americana por forma a compatibilizar este meio de obtenção de prova com os direitos dos cidadãos.

Assim, seguindo Susan Brenner, o mandado tem de ser fundado numa causa provável, isto é, em factos e circunstâncias que permitam criar uma convicção sustentada que determinado elemento de prova pode ser encontrado no computador do visado. Neste contexto, é essencial identificar o ilícito criminal em investigação, o local da busca e os objetos visados, bem como os dados que se visam apreender nesse período do mandado (Brenner, 2011).

---

[67] Mais detalhes em: https://www.elconfidencial.com/tecnologia/2020-07-03/encrochat-red-social-criminal-sito-minanco-europol_2667831/ (Consultado a 01/11/2020).

[68] O art. 41.º do *Federal Rules of Criminal Procedure* está acessível em https://www.federalrulesofcriminalprocedure.org/title-viii/rule-41-search-and-seizure/ (Consultado em 01/11/2020).

3. SOLUÇÕES ADOTADAS EM PAÍSES EUROPEUS

Tendo-se abordado a utilização do *malware* ou *benware*, na expressão recente de Duarte Rodrigues Nunes, quando está em causa a utilização, por parte das autoridades de programas informáticos para fins de prevenção ou repressão criminais (Nunes D. R., 2020), como meio de obtenção de prova eficaz na recolha de prova digital, salientou-se também o seu vasto potencial, visto ser possível não só copiar a informação de um determinado sistema informático, num único ato, mas também e de forma contínua monitorizar esse sistema informático, bem como ativar os microfones, a *webcam* e registar a utilização do teclado.

Após se ter efetuado uma breve resenha histórica da utilização destes meios tecnológicos nos E.U.A, procurar-se-á, agora, analisar algumas das especificidades da consagração deste meio de obtenção de prova em países europeus, colocando o enfoque na sua utilização no âmbito das denominadas buscas *online*, em sede de investigação criminal, com a convicção que esta figura será essencial na redefinição da pesquisa de dados informáticos, enquanto meio de obtenção de prova no nosso ordenamento jurídico.

Para tal, abordar-se-á, ainda que de forma sumária, o ordenamento jurídico alemão, espanhol e francês.

3.1. ALEMANHA

Na Alemanha, a pesquisa de dados informáticos encontra-se consagrada na secção 110 (3) do StPO[69], salientando-se que, à semelhança do que sucede na Lei do Cibercrime nacional, esta pesquisa pode ser estendida a outros sistemas informáticos, quando acessíveis a partir do sistema inicial e existam fundadas razões para crer que esses dados informáticos possam ser perdidos.

No que concerne à utilização de *malware*, no âmbito das investigações criminais, constata-se a sua consagração no StPO (*Strafprozessordnung*).

[69] O Código de Processo Penal Alemão (Strafprozessordnung – StPO) está disponível em: https://www.gesetze-im-internet.de/ (Consultado a 15/11/2020).

Deste modo, o § 100a, que se refere à interceção de comunicações, prevê a utilização de meios técnicos necessários à interceção e gravação das comunicações antes da mesmas serem encriptadas ou depois de serem desencriptadas (Directorate General For Internal Policies, 2017, p. 79) e o § 100b, prevê a possibilidade de pesquisa remota (*Online-Durchsuchung*), sem o conhecimento do visado, a um sistema informático, com vista a extrair dados desse sistema.

Ir-se-á analisar com maior detalhe o regime da pesquisa remota, sem o conhecimento do visado.

Começando pelo âmbito da aplicação desta norma, constata-se que o § 100b do StPO permite a utilização destes meios quando está em causa a prática de crime particularmente grave, encontrando-se este conceito devidamente densificado no catálogo de crimes constante do § 100b (2) dessa secção. Evidencia-se ainda que, além de um âmbito de aplicação restringido, estes meios apenas poderão ser utilizados, caso seja "muito difícil ou impossível alcançar o mesmo resultado através de outro meio de obtenção de prova menos gravoso" (Batista, 2018, p. 53).

No que concerne à competência para autorização da utilização deste meio de obtenção de prova, estabelece o § 100e que o mesmo é autorizado, após requerimento do MP, por três juízes da Secção Criminal do *Landgericht* (Tribunal estadual de 2ª instância) da área da sede do departamento do MP competente para a investigação, ou, em situações de urgência, pelo Presidente dessa Secção Criminal, sendo depois necessária a ratificação por parte de três juízes da Secção Criminal no prazo de três dias úteis (Nunes D. R., 2020).

A utilização deste meio de obtenção de prova fica limitada à duração máxima de um mês, podendo também ser prorrogado por idêntico período, caso subsistam os fundamentos que determinaram a emissão do despacho a ordenar a utilização do referido meio de obtenção de prova (*Ibidem*).

Relativamente ao teor do despacho a ordenar a aplicabilidade deste meio de obtenção de prova, o § 100b do StPO, refere que o mesmo terá de indicar os factos concretos que originaram as suspeitas, bem como a justificação da necessidade e proporcionalidade da medida. Deverá ainda constar, na medida

do possível, o nome e morada do visado; a base legal para aplicação do meio de obtenção de prova; a finalidade e a duração desta medida; tipo de informação que se pretende obter e a sua importância para a investigação; exige-se ainda uma descrição, o mais precisa possível da forma como os dados serão obtidos (*Ibidem*).

Destaca-se também a preocupação vertida nesta norma legal no que tange ao núcleo central da vida privada do visado, estabelecendo-se a impossibilidade de recolha destes dados, que não podem ser utilizados e deverão ser eliminados.

3.2. ESPANHA

Em Espanha a pesquisa de dados informáticos encontra-se prevista, desde dezembro de 2015, na *Ley de Enjuiciamiento Criminal*[70], mais precisamente no Título VIII, Capítulo VIII, art.º 588, tratando-se de um meio de obtenção de prova, cujo regime, no essencial, é idêntico ao previsto na Lei do Cibercrime.

Com efeito, a utilização deste meio carece de autorização judicial, destacando-se ainda o disposto no n.º 3 do artigo 588 *sexies c.*, segundo o qual se permite estender a pesquisa a outros sistemas informáticos, quando haja motivo para crer que os dados suscetíveis de interessar à investigação aí se encontrem e os mesmos possam ser acedidos através do sistema inicial, à semelhança do previsto no art.º 15.º, n.º 5 da Lei do Cibercrime.

Todavia, a *Ley de Enjuiciamiento Criminal* vai mais longe ao consagrar, tal como no ordenamento jurídico alemão, no artigo 588 *septies*, a possibilidade de aceder remotamente e sem o conhecimento do visado ao conteúdo dos sistemas informáticos por este utilizados ou dos suportes externos de armazenamento em massa de dados informáticos, designadamente através da instalação de *software (registros remotos sobre equipos informáticos).*

[70] Este diploma legal pode ser acedido em: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036#tviii-2 (Consultado a 16/11/2020).

Estes meios poderão ser utilizados, nos termos do n.º 1 do artigo 588 *septies,* nomeadamente na investigação de crimes de terrorismo ou cometidos no seio de organizações terroristas, bem como crimes cometidos contra menores ou incapazes, relativos à defesa nacional e crimes cometidos através de meios informáticos.

O despacho judicial a autorizar a utilização destes meios, nos termos do n.º 2 do referido artigo, deve especificar: os dispositivos visados; a forma como os dados serão acedidos e apreendidos; o *software* que permitirá executar o controlo dessa informação; os agentes autorizados a executar esse meio de obtenção de prova; autorização, caso seja necessário, para realizar cópia dos dados informáticos, bem como as medidas necessárias para garantir a preservação da integridade dos dados.

Este meio de obtenção de prova terá a duração máxima de um mês, prorrogável por iguais períodos até ao máximo de três meses (artigo 588, *septies* c.).

Destaca-se ainda que os meios de obtenção de prova anteriormente referidos terão de observar os princípios orientadores que se encontram elencados no artigo 588 *bis* a.: especialidade, idoneidade excecionalidade, necessidade e proporcionalidade da medida.

Assim, o princípio da especialidade exige que a medida a ser utilizada esteja relacionada com a investigação de um determinado crime. O princípio da idoneidade servirá para definir o alcance da medida e a duração da mesma em função da sua utilidade. Os princípios da excecionalidade e da necessidade implicam que o meio de obtenção de prova apenas pode ser utilizado quando outras medidas menos onerosas para os direitos fundamentais do visado não se afigurem adequadas, ou quando a descoberta da verdade ou identificação do(s) autor(es) dos factos em investigação fique gravemente prejudicada sem o recurso a essa medida. Por fim, o princípio da proporcionalidade exige ainda a ponderação entre o sacrifício dos direitos e interesses afetados e os benefícios da adoção de determinado meio de obtenção de prova para o interesse público e terceiros.

O elenco e definição destes princípios evidenciam que a ingerência do Estado no direito à privacidade dos cidadãos está sujeita a limites devidamente clarificados e com controlo efetivo, sendo que a consagração da possibilidade de aceder remotamente a um sistema informático, sem o conhecimento do visado, assume-se como um meio de caráter excecional, embora se reconheça a sua necessidade para a investigação de determinados crimes, desde que a adoção de outros meios de obtenção de prova menos invasivos não permitam alcançar os mesmos resultados (Winter, 2017).

3.3. FRANÇA

No ordenamento jurídico francês, a pesquisa de dados informáticos encontra-se prevista no art.º 57-1 do *Code de procédure pénale*[71], estabelecendo-se que os agentes da Polícia, durante uma busca podem aceder aos dados de um sistema informático, permitindo-se ainda estender essa busca a outros sistemas informáticos, desde que os dados sejam acessíveis a partir do sistema inicial. Todavia, no âmbito do terceiro parágrafo desta norma estabelece-se, expressamente, uma limitação que convém sublinhar. Assim, caso os dados acessíveis, através do sistema inicial, se encontrem armazenados noutro sistema informático situado fora do território nacional, os dados para serem recolhidos terão de observar as condições de acesso previstas nos acordos internacionais em vigor.

Se é verdade que esta limitação poderá restringir de forma evidente o âmbito da pesquisa de dados informáticos, também é verdade que à semelhança do que se encontra previsto na legislação alemã e espanhola, também o ordenamento jurídico francês prevê o recurso ao *malware*.

Com efeito, o artigo 706-102-1, refere a possibilidade de se aceder a dados informáticos, com possibilidade de os guardar e transmitir, especificando ainda que esses dados poderão estar armazenados num sistema informático, bem como os que são exibidos no ecrã para o utilizador, incluindo os que vão sendo introduzidos ou recebidos.

[71] Este diploma legal encontra-se acessível em: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/ (Acedido a 17/11/2020).

No *Code de procédure pénale* destaca-se ainda que este meio de obtenção de prova só deverá ser instalado fisicamente, nos termos do artigo 706-12.5, o que apresenta desde logo a vantagem de evitar que este meio atinja pessoas que não o visado. No entanto apresenta a desvantagem de ser necessário conhecer a localização física desse sistema informático (Batista, 2018).

No que diz respeito à competência para implementar a utilização destes meios, no âmbito da investigação, cabe ao juiz das liberdades e da detenção a pedido do MP.

A decisão que autoriza o uso deste meio de obtenção de prova terá de especificar a infração que fundamenta a sua utilização, a localização exata ou a descrição detalhada dos sistemas informáticos, bem como a duração das operações. Esta autorização, para a investigação, é emitida pelo prazo máximo de um mês, podendo ser renovada por idêntico período.

Quanto ao catálogo de infrações relativamente às quais se pode utilizar este meio de obtenção de prova, o mesmo consta dos artigos 706-73 e 706-73-1, por força do disposto no art.º 706-95-11, tratando-se de crimes graves e, designadamente, praticados de forma organizada.

Também se refere a necessidade de elaboração de um relatório onde se faça menção aos elementos suscetíveis de terem utilidade para o esclarecimento da verdade material dos factos.

Compulsados, ainda que de forma breve, estes ordenamentos jurídicos é possível extrair as seguintes conclusões: a pesquisa de dados informáticos, sem o conhecimento do visado, usando para o efeito meios informáticos instalados sub-repticiamente nos sistemas informáticos é de utilização excecional, consubstanciando um meio de *ultima ratio*; o seu regime encontra-se previsto de forma clara e detalhada, estando associado a um catálogo restrito de crimes; exige-se ainda autorização judicial, cujo despacho deverá ser devidamente fundamentado e a sua utilização limitada a períodos temporais curtos.

4. A PESQUISA DE DADOS INFORMÁTICOS - LIMITAÇÕES

No âmbito do presente estudo analisou-se os meios de obtenção de prova, previstos nos artigos 12.º a 19.º, da Lei do Cibercrime, com especial enfoque na pesquisa de dados informáticos.

Seguidamente, procurou-se conhecer as soluções da Ciência Forense Digital para a recolha de prova digital, alicerçada em princípios atinentes à custódia da prova, salientando-se as soluções tecnológicas que permitem superar as medidas anti-forenses adotadas, tais como a encriptação, que vêm sendo generalizadas e colocam sérios entraves às autoridades no âmbito da realização de diligências tendentes à obtenção de elementos probatórios.

Destas soluções tecnológicas destacou-se a utilização do *malware*, pelo seu potencial de eficácia e aplicabilidade, designadamente em pesquisas de dados remotas, sem o conhecimento do visado, estando atualmente a sua utilização consagrada em diversos ordenamentos jurídicos tais como nos E.U.A, Alemanha, Espanha e França.

Chegados aqui, importa agora ponderar se a pesquisa de dados informáticos, tal como se encontra prevista no art.º 15.º Lei do Cibercrime se afigura um meio adequado de recolha de prova digital, atendendo aos avanços tecnológicos, entretanto, ocorridos. Caso se conclua pela negativa, procurar-se-á analisar a admissibilidade da pesquisa remota de dados informáticos, sem o conhecimento do visado, face aos valores jurídico-constitucionais vigentes no nosso ordenamento jurídico, esperando-se também que deste labor resultem critérios axiológicos que permitam perceber em que medida se poderá redefinir a pesquisa de dados informáticos enquanto importante meio de obtenção de prova no combate a uma criminalidade cada vez mais sofisticada.

Não se afigura uma tarefa fácil a conciliação e subsunção de novas formas de aquisição probatória, inseridas numa realidade tecnológica em constante mutação, com as previsões legais da Lei do Cibercrime que não sofreu qualquer alteração desde a data da sua publicação. No entanto, “é através da investigação que se reflete e problematizam os problemas nascidos na prática, que se suscita o debate e se edificam as ideias inovadoras.” (Coutinho, 2014, p. 6).

A pesquisa de dados informáticos, conforme já se referiu, não é um meio de obtenção de prova de *ultima ratio*, diversamente do que sucede com interceção de comunicações ou as ações encobertas, constituindo até um meio habitual de recolha de prova digital. Tanto assim é que, da conjugação do disposto no art.º 15.º com o art.º 11.º, n.º 1, alíneas a) e c), da Lei do Cibercrime, não existe qualquer catálogo de crimes que lhe esteja associado. Ainda assim, este meio de obtenção de prova implicando o acesso a dados informáticos de qualquer natureza, restringe os direitos à intimidade e privacidade, à palavra virtual (art.º 26.º), à autodeterminação informacional (art.º 35.º) e à inviolabilidade das comunicações (art.º 34.º da CRP)[72].

Acerca do grau de suspeita para fundamentar a sua utilização, no âmbito da investigação criminal, verifica-se que o regime legal da pesquisa de dados informáticos não prevê qualquer exigência a este respeito, "sendo suficiente uma suspeita inicial objetivável" (Nunes D. R., 2018, p. 96).

Por último, importa novamente salientar que a competência para autorizar a pesquisa de dados informáticos, nos termos do art.º 15.º, n.º 1 da Lei do Cibercrime cabe à autoridade judiciária competente, ou seja, ao magistrado do Ministério Público, na fase de inquérito, ao JIC, na fase da instrução e ao juiz na fase de julgamento (*Idem*, p. 101).

Uma vez emitido esse mandado e no âmbito do cumprimento do mesmo, as autoridades deparam-se com sistemas informáticos protegidos por vários métodos de autenticação, baseando-se os mesmos nos seguintes princípios: princípio do conhecimento: algo que a pessoa sabe (*password*, padrão PIN); princípio da posse: algo que a pessoa tem (*exemplo* do *token*, dispositivo eletrónico que gera chaves) e princípio da identidade: algo que a pessoa é ou faz (impressão digital, a íris, ou o rosto)[73].

Não raras vezes, também se deparam, cumulativamente, com os meios anteriormente enunciados, com sistemas informáticos protegidos por encriptação.

[72] Conforme bem salienta Duarte Nunes (Nunes D. R., 2018, p. 95).
[73] Conforme explicado por Vanessa Fernandes (Fernandes, 2018, p. 64).

A encriptação, conforme já se ressaltou, constitui um obstáculo técnico, na maior parte das vezes, intransponível para os órgãos de polícia criminal, que ficam dependentes da boa vontade do suspeito para aceder aos sistemas informáticos que estiverem na sua posse.

Assim sendo, a questão que se coloca é se poderá ser imposto ao suspeito o fornecimento da informação que possibilite o acesso ao sistema informático (*password*, padrão ou PIN) ou a aposição da sua impressão digital, íris ou rosto, por exemplo, a fim de se concretizar a pesquisa de dados informáticos.

Ora esta questão surge diretamente relacionada com o respeito pela dignidade da pessoa humana, sendo importante analisar no âmbito desta temática o princípio da lealdade na atuação policial e o princípio da não autoincriminação, também conhecido como *nemo tenetur se ipsum accusare,* bem com as implicações dos mesmos no âmbito da recolha de prova digital.

4.1. A POLÍCIA E OS DIREITOS FUNDAMENTAIS

Não se perdendo de vista as relações de "interpenetração que medeiam entre a Constituição e o processo penal, traduzidas na conhecida síntese de Henkel: o direito processual penal como verdadeiro direito constitucional aplicado" (Costa Andrade, 2013, p. 12), iniciar-se-á a presente abordagem pelo art.º 32.º, n.º 8 da CRP que estabelece que *são nulas todas as provas obtidas mediante tortura, coação, ofensa à integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicilio, na correspondência ou nas telecomunicações.*

Com efeito, é no âmbito deste artigo que se "condensam os mais importantes princípios materiais de processo criminal – a constituição processual criminal" (Canotilho & Moreira, 2007, p. 515).

Não é despiciendo evidenciar que o instituto das proibições de prova assume no ordenamento jurídico português dignidade constitucional, não obstante também existir uma norma respeitante aos métodos proibidos de prova

no art.º 126.º do CPP. Assim sendo, os interesses do processo penal, nomeadamente no que concerne ao alcance da verdade material dos factos, "encontra limites na dignidade da pessoa humana (art.º 1.º da CRP), e nos princípios fundamentais do Estado de direito democrático (art.º 2.º), não podendo, portanto, valer-se de atos que ofendam direitos fundamentais básicos" (Canotilho & Moreira, 2007, p. 524).

Com efeito, o art.º 18.º, n.º 1 da CRP estabelece de forma perentória que *os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são diretamente aplicáveis e vinculam as entidades públicas e privadas*". Por sua vez, o n.º 2 deste artigo estabelece que *a lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos*.

Relativamente ao n.º 1 do artigo 18.º evidencia-se, desde logo, caber nas funções da Polícia, nos termos do art.º 272.º, n.º 1 da CRP *defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos*.

Deste modo, os direitos dos cidadãos não constituem apenas um limite à atuação da Polícia, mas também um dos fins inerentes à sua função (Canotilho & Moreira, 2007).

No que diz respeito à última parte do n.º 2 do artigo 18.º, correlacionando o mesmo com o n.º 2 do art.º 272.º, importa evidenciar outra garantia de limitação do poder público e, por conseguinte, da atuação Policial.

Assim sendo, não só o artigo 272.º n.º 2 consagra a tipicidade legal dos atos de Polícia, como também determina que esses atos não devem ser utilizados para além do estritamente necessário, numa evidente reafirmação do princípio da proporcionalidade no que tange às restrições aos direitos, liberdades e garantias, previsto no art.º 18.º, n.º 2.

Este princípio, conforme ensina Gomes Canotilho e Vital Moreira, subdivide-se no princípio de adequação, segundo o qual as medidas restritivas de direitos, liberdades e garantias, devem configurar um meio idóneo à prossecução dos fins visados pela lei, fins esses de tutela de outros direitos ou interesses também constitucionalmente protegidos; no princípio da exigibilidade

ou necessidade, que significa que as medidas restritivas têm que ser necessárias, porquanto inexistem outras menos onerosas para os direitos, liberdades e garantias aptas a alcançar o fim visado; e, no princípio da proporcionalidade em sentido estrito, que postula uma "justa medida" entre essas medidas restritivas e os fins pretendidos (Canotilho & Moreira, 2007, pp. 392-393).

Da correlação destes preceitos constitucionais com o artigo 126.º do CPP resulta a formulação do princípio da lealdade na obtenção de provas, que segundo Germano Marques da Silva implica que a "eficácia da justiça é (…) um valor que deve ser perseguido, mas, porque numa sociedade livre e democrática os fins nunca justificam os meios". Acerca da temática que agora é objeto de análise refere ainda que o "moderno desenvolvimento dos métodos científicos de investigação recolocou a problemática do respeito pela dignidade das pessoas em termos tão prementes como relativamente a alguns dos métodos bárbaros do passado" (Silva, 2000, pp. 67, 68).

4.2. *NEMO TENETUR SE IPSUM ACCUSARE*

O princípio da não autoincriminação, também conhecido como *nemo tenetur se ipsum accusare* é outro dos princípios fundamentais, que consubstancia uma importante limitação à recolha da prova digital e, por conseguinte, à atuação policial no âmbito da investigação criminal.

Este princípio, segundo Sousa Mendes, relaciona-se também com a garantia de um processo justo e equitativo, conforme previsto no art.º 24.º da CRP e assenta na ideia de que "ninguém deve ser obrigado a contribuir para a sua incriminação" englobando este princípio o direito ao silêncio e o direito de não facultar meios de prova (Mendes, 2013, p. 209).

Também na esteira do que é ensinado por Costa Andrade, o privilégio da não autoincriminação assenta na liberdade de declaração, numa dupla dimensão: negativa e positiva. A dimensão positiva está relacionada com o

direito que assiste ao arguido de intervir ou prestar declarações em sua defesa. A dimensão negativa, consubstancia uma garantia que veda:

> Todas as tentativas de obtenção, por meios enganosos ou por coação, de declarações autoincriminatórias (…) O que está aqui fundamentalmente em jogo é garantir que qualquer contributo do arguido, que resulte em desfavor da sua posição, seja uma afirmação esclarecida e livre de autorresponsabilidade (*Ibidem*, p. 121).

Não obstante não estar expressamente previsto na Constituição, entende a doutrina e a jurisprudência ser inquestionável que este princípio tem consagração constitucional, como referido desde logo no Ac. TC n.º 155/2007, de 02/03/2007[74] e também como salienta Costa Andrade (Costa Andrade, 2013, p. 125).

O Tribunal Constitucional evidencia ainda a importância do princípio da não autoincriminação, enquanto princípio basilar de um processo penal de estrutura acusatória, que está ínsito nas garantias consagradas no art.º 32, n.º 1 da CRP, sendo certo que, reflexamente, também tutela a dignidade da pessoa humana, ao não reduzir o arguido "a um mero objeto da atividade estadual de repressão do crime, devendo antes ser-lhe atribuído o papel de verdadeiro sujeito processual, armado com os direitos de defesa e tratado como presumivelmente inocente" (Ac. TC n.º 340/2013, de 17/06/2013)[75].

Prossegue ainda este acórdão, evidenciando que o princípio da não autoincriminação manifesta-se no âmbito do processo penal desde logo de forma preventiva, isto é, vedando soluções que impliquem a obrigatoriedade do arguido fornecer elementos de prova que possam contribuir para a sua condenação, bem como de forma repressiva, determinando a desconsideração de elementos de prova obtidos através de uma "colaboração imposta ao arguido".

No entanto, se a sua matriz constitucional é pacífica, a "definição da sua compreensão e alcance (…) a precisa demarcação da respetiva área de tutela suscita dificuldades" (Costa Andrade, 2013, p. 127).

---

[74] http://www.tribunalconstitucional.pt/tc/acordaos/20070155.html (acedido a 19/11/2020).
[75] Este acórdão pode ser consultado em: http://www.tribunalconstitucional.pt/tc/acordaos/20130340.html (acedido a 19/11/2020).

Estas dificuldades são patentes na "zona de fronteira e concorrência entre o estatuto do arguido como sujeito processual e o seu estatuto como objeto de medidas de coação ou de meios de prova"[76].

Tanto assim é que o Tribunal Constitucional reconhece, no já citado Ac. TC 340/2013, de 17/06/2013, que "o direito à não incriminação não tem caráter absoluto, podendo ser legalmente restringido em determinadas circunstâncias (por exemplo a obrigatoriedade de realização de determinados exames ou diligências que exijam a colaboração do arguido, mesmo contra a sua vontade)"[77].

Não se olvide que já em 2007, no âmbito do referido acórdão do TC n.º 155/2007, o Tribunal Constitucional já tinha declarado, acompanhando a decisão do TEDH, em sentença proferida em 17/12/1996 (caso *Sauders* c. Reino Unido), que o "direito à não incriminação, se refere ao respeito pela vontade do arguido, não abrangendo (…) o uso em processo penal, de elementos que se tenham obtido do arguido por meio de poderes coercivos, mas que existam independentemente da vontade do sujeito"[78].

Importa ainda destacar o Acórdão do TEDH, de 11/07/2006 (caso Jalloh c. Alemanha) pelos critérios enunciados com vista a aferir a violação do princípio *nemo tenetur se ipsum accusare.*

Segundo este acórdão, citado por Sousa Mendes:

> Para determinar se o direito à não incriminação do queixoso foi violado, o Tribunal, por sua vez, terá de considerar os seguintes fatores: a natureza e o grau de coerção empregado para obter as provas, a importância do interesse público na investigação e punição da infração em apreço, a existência de garantias relevantes no processo e a utilização prevista dos meios de obtenção de prova obtidos dessa forma" (Mendes, 2013, p. 215).

[76] Conforme é referido no Ac. do TC. *Vide* nota de rodapé n.º 74.
[77] *Vide* nota de rodapé n.º 75.
[78] O tribunal Constitucional refere como exemplo a colheita de saliva para efeitos de realização de análises de ADN.

Estes arestos permitem perceber que o direito à não autoincriminação não é um direito absoluto, admitindo exceções, que devem ser casuisticamente ponderadas, no confronto com outros interesses juridicamente protegidos.

Também a doutrina maioritária reconhece que o direito à não incriminação não é absoluto, admitindo que o mesmo possa ser restringido. Todavia, essa restrição tem que assentar em dois pressupostos: a existência de uma lei prévia, nos termos exigidos pelo princípio da legalidade, visto que, como bem refere Costa Andrade "todo o atentado à liberdade dos cidadãos carece de expressa legitimação legal" (2013, p. 130), devendo ainda obedecer ao princípio da proporcionalidade que decorre do art.º 18.º, n.º 2.

Face ao que foi exposto, compulsada a Lei do Cibercrime desde logo nos deparamos com o art.º 14.º, que se reporta à injunção para apresentação ou concessão do acesso a dados, sendo que o n.º 5 deste artigo estabelece, de forma inequívoca que *a injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo.*

Assim sendo, terá que se concluir, como o faz Vanessa Fernandes, que qualquer ordem no sentido do suspeito ou arguido revelar a palavra-passe ou apor a impressão digital de modo a permitir o acesso a um sistema informático, será ilegítima por violação do princípio *nemo tenetur se ipsum accusare* (Fernandes, 2018)[79].

4.3. PESQUISA DE DADOS REMOTA SEM O CONHECIMENTO DO VISADO

Do que se expôs anteriormente, constata-se que a obtenção de prova através da pesquisa de dados informáticos poderá ficar completamente inviabilizada, no caso de um sistema informático se encontrar protegido por meio de encriptação, não existindo também qualquer norma no ordenamento jurídico que permita compelir o visado a revelar as credenciais de acesso a um determinado sistema informático.

[79] A este respeito salienta-se o facto de existirem ordenamentos jurídicos, tais como o Reino Unido e belga, onde se encontra prevista a criminalização da recusa em fornecer a *password* (Fernandes, 2018, pp. 131-132).

Ciente destas limitações, a Ciência Forense Digital tem vindo a oferecer soluções que permitem ultrapassar estas dificuldades, tendo vários ordenamentos jurídicos plasmado as mesmas, designadamente em meios de obtenção de prova já previstos, aumentando desta forma o seu alcance e eficácia.

Assim sendo, o que importa agora analisar, de forma mais detalhada, é se a pesquisa de dados informáticos, de forma remota, sem o conhecimento do visado, também designada pela doutrina como *Busca Online* é admissível no âmbito do ordenamento jurídico português.

A busca *online* reconduz-se ao recurso a programas informáticos, tais como os cavalos de tróia, instalados sub-repticiamente no sistema informático do visado, com vista à recolha de prova. Esta busca pode consistir num único acesso (*Daten-Spiegelung*) ou ocorrer de forma contínua e prolongada no tempo (*Daten-Monitoring*) (Nunes D. A., 2019).

Na discussão na generalidade da proposta de Lei n.º 289/X/4ª, que veio dar origem à Lei do Cibercrime, o Deputado Fernando Negrão, do Grupo Parlamentar do Partido Social Democrata questionou:

> Porque é que não foi contemplada neste diploma a possibilidade de as entidades de investigação criminal introduzirem em determinado sistema que esteja sob investigação o que podemos designar por "cavalo de Tróia informático" para poder obter informação contínua e em tempo real, assim facilitando as investigações criminais (DAR I série n.º 102/X/4 2009.07.10, p. 40)[80].

Não obstante a questão colocada, esta proposta não sofreu qualquer alteração com vista a admitir a utilização destes recursos tecnológicos.

Ainda assim, segundo Paulo Pinto de Albuquerque, as buscas *online* teriam sido consagradas no art.º 15.º da Lei do Cibercrime. Todavia, esta norma suscita problemas de inconstitucionalidade, face ao disposto nos artigos 26.º n.º 1 e 2 e 32.º n.º 4 da CRP, que reservam ao juiz os atos instrutórios que se

[80] Acessível a partir de: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?ID=34566 (Consultado a 20/11/2020).

prendem diretamente com direitos fundamentais. No entanto, a obtenção de dados pessoais ou íntimos estaria salvaguardada pela intervenção posterior do juiz, que ponderaria a sua junção aos autos, tendo em conta os interesses do caso concreto, *ex vi* art. 16.º n.º 3 da Lei do Cibercrime (Albuquerque, 2011).

Por sua vez, a posição de Duarte Rodrigues Nunes assenta na distinção entre um único acesso (*Daten-Spiegelung*) ou acesso de forma contínua e prolongada no tempo (*Daten-Monitoring*). Tratando-se de um único acesso e não exigindo o art.º 15.º da Lei do Cibercrime que a pesquisa seja presencial, a busca online poderá ser realizada em obediência ao princípio *ubi lex no dintinguit nec nos distinguere debemus* (Nunes D. R., 2020, p. 35).

> Nos casos em que a infiltração no sistema informático seja levada a cabo de forma contínua e prolongada no tempo (*Daten-Monitoring*), o art.º 15.º deve ser interpretado de forma hábil, de molde a apenas serem admissíveis buscas *online* nos casos em que fosse admissível lançar mão da intervenção nas comunicações eletrónicas nos termos do art.º 18.º da Lei do Cibercrime, aplicando-se *mutatis mutandis* o respetivo regime jurídico (*Idem*, p. 40).

Evidencia-se, no entanto, que não obstante a posição defendida por este autor, o mesmo também refere que, de forma a dissipar as dúvidas, o legislador português deveria prever este meio de obtenção de prova expressamente, à semelhança do que foi feito pelos legisladores espanhol e alemão (*Ibidem*).

Defendendo a posição da inadmissibilidade deste meio de obtenção de prova no ordenamento jurídico português, Rita Castanheira Neves enfatiza que a *busca online* é "altamente lesiva da privacidade da pessoa – que deposita, hoje em dia, quase todos os passos da sua vida no computador", pelo que teria "que se sujeitar a regras, requisitos de admissibilidade, formalidades especiais, e, sobretudo, respeitar rigidamente os princípios da necessidade, subsidiariedade e proporcionalidade" (Neves, 2011, p. 196).

Também Silva Ramalho defende que o *malware*, cuja instalação, *a priori*, é necessária para a realização de buscas *online,* deverá "cumprir integralmente

os requisitos de reserva de lei e de densificação legal, proporcionalidade, subsidiariedade" (…) assegurando "devidamente o direito ao contraditório e o respeito pelas garantias de defesa do visado" (Ramalho, 2017, p. 352).

Trata-se aqui de ter presente, desde logo, os princípios norteadores ínsitos no art.º 18.º da CRP, em termos de restrição de direitos fundamentais, que se manifestam no brocardo latino *Odiosa sunt restringenda* (Gouveia, 2020) e que já foram abordados, dos quais se destaca a exigência de reserva de lei.

Em termos de análise da jurisprudência relacionada com este tema e de forma a encontrarem-se critérios axiológicos, conformes com a Constituição, esta tem vindo também a exigir uma densidade normativa suficiente às normas restritivas de direitos fundamentais. Com efeito, resulta do acórdão do TC n.º 155/2007[81] que, sustentando-se nas palavras de Vieira de Andrade, refere o seguinte:

> A lei restritiva, em função da reserva de lei formal, tem de apresentar uma densidade suficiente, isto é, um certo grau de determinação do seu conteúdo, pelo menos no essencial, não sendo legítimo que deixe à Administração espaços significativos de regulação ou de decisão.

Também se estribando em Jorge Reis Novais refere que:

> Com leis suficientemente claras e determinadas se garante que é o próprio legislador que toma as decisões essenciais, as exigências de segurança próprias de um Estado de direito, bem como o direito à tutela judicial efetiva do direito fundamental afetado, uma vez que da densidade normativa da regulamentação legal depende também, em alguma medida, a adequação funcional da intensidade variável do controlo judicial da atividade administrativa.

Estas exigências de clareza e determinabilidade dos meios de obtenção de prova, em especial em ambiente digital, pelo potencial lesivo dos direitos dos cidadãos, são corolário do princípio da legalidade, previsto no art.º 29.º da CRP

[81] *Vide* nota de rodapé 72.

que, como se sabe, assumiu no pensamento iluminista-liberal, de finais do século XVIII, a garantia da segurança do cidadão contra o arbítrio do Estado, ou como elucida Fernanda Palma "é expressão da autolimitação do Estado perante os cidadãos e da sua função primordial de proteção da pessoa" (Palma, 2018, p. 126).

Por último, não se pode deixar de salientar que a exigência de previsão legal, de forma clara e detalhada, também vai de encontro à jurisprudência do TEDH. Com efeito, já na decisão proferida a 02/08/1984 (caso Malone c. Reino Unido), se referia que:

> A lei deve usar termos suficientemente claros para indicar a todos, de maneira suficiente, em que circunstâncias e em que condições as autoridades públicas têm poderes para recorrer a esta interferência secreta e virtualmente perigosa, ao direito ao respeito pela vida privada e da correspondência (Ramalho, 2017, p. 342).

Também na decisão proferida a 02/09/2010 (caso Uzun c. Alemanha), a propósito da obtenção de dados de localização, através de GPS, o Tribunal considerou que este meio de obtenção de prova era suscetível de violar o direito ao respeito da vida privada e familiar, do domicílio e da correspondência, garantidos pelo art. 8.º da CEDH. Deste modo, evidenciou que "por causa do risco de abuso intrínseco a um sistema de vigilância oculta, tais medidas carecem de uma habilitação legal particularmente precisa, especialmente quando a tecnologia se torna progressivamente mais sofisticada" (Brito, 2018, pp. 52-53). *In casu*, o ordenamento jurídico alemão dispunha de uma norma que "constituia base legal suficiente e que era compreensível para os seus destinatários" (Nunes D. R., 2019, p. 10).

No âmbito da mesma temática e, mais recentemente, no âmbito da decisão do TEDH de 08/02/2018 (caso Ben Faiza c. França), o Tribunal, contrariamente à decisão anterior, entendeu que o acesso à localização do veículo em tempo real, através de GPS, consubstanciava uma violação do art.º 8.º da CEDH, porquanto a norma prevista no ordenamento jurídico francês à data dos factos "não indicava com suficiente clareza e precisão as condições e os

limites de aplicação do GPS enquanto método de obtenção de prova" (Brito, 2018, p. 60).

Nesta sequência, regressando ao enquadramento do *malware* utilizado no âmbito das investigações criminais, em especial como forma de concretizar pesquisas de dados informáticos sem o conhecimento do visado, é forçoso concluir que este tipo de meios, ocultos ao visado, "estão sujeitos a exigências, particularmente rígidas de reserva de lei, só sendo admitidos na medida em que gozem de expressa, específica e detalhada consagração, obviamente não admitindo o recurso à analogia" (Brito, 2018, p. 50).

Particularmente importantes sobre esta temática são os pressupostos enunciados por Costa Andrade, que devem ser observados pela lei sobre métodos ocultos de investigação: o "catálogo de crime, grau de suspeita, subsidiariedade, autorização/ordenação pela autoridade competente e informação da pessoa atingida depois de terminada a medida" (Costa Andrade, 2009, p. 545.). Estas "variáveis", na expressão deste autor, devem ser norteadas pelo princípio da proporcionalidade, exigindo-se ainda uma ponderação, no sentido de aferir se a gravidade da medida a ser aplicada não é desproporcionada face às finalidades de uma determinada investigação (Rodrigues, 2011).

Do que foi exposto anteriormente, não se suscitam dúvidas relativamente à abertura constitucional para a consagração deste importante meio de obtenção de prova que servirá para complementar as grandes limitações da pesquisa de dados informáticos, tal como prevista na Lei do Cibercrime. Sufraga-se a este respeito a opinião de Conde Correia de que "a luta contra formas extremas da criminalidade, que põem em perigo a manutenção do próprio Estado de direito, deve poder contar – insistimos de novo – com esta possibilidade suplementar" (Conde Correia, 2014, p. 44).

Assim sendo, defende-se a perspetiva de que urge consagrar a busca *online* de forma clara e detalhada à semelhança do que sucede na Alemanha, Espanha e França.

4.4. *DE IURE CONDENDO*

A construção de uma norma legal tendente a regular de forma expressa e detalhada a pesquisa de dados remota sem o conhecimento do visado, não se afigura fácil. No entanto, entende-se que chegados a este momento estar-se-á em condições de avançar critérios norteadores, na construção de uma norma habilitante, que permitam enquadrar este meio de obtenção de prova.

Deste modo, assumindo-se aprioristicamente que se encontra cumprida a exigência de reserva de lei, clara e detalhada, dir-se-á também que esta norma deverá revestir caráter excecional e de *ultima ratio*, devendo ser circunscrita aos casos em que o meio de obtenção de prova é indispensável para a descoberta da verdade ou quando a recolha da prova seria impossível ou muito difícil de obter.

Deverá ainda ser ponderado um catálogo de crimes graves, no âmbito dos quais este meio de obtenção de prova pode ser utilizado, à semelhança do que sucede, por exemplo, com a Lei 5/2002, de 11 de janeiro, que estabelece um regime especial de recolha de prova, no âmbito das medidas de combate à criminalidade organizada e económico-financeira.

No que concerne à autorização para a utilização deste meio de obtenção de prova, a mesma caberá ao juiz, através de despacho devidamente fundamentado.

O controlo dos elementos de prova obtidos poderá ser realizado à semelhança do previsto nas interceções telefónicas, de forma a garantir o contraditório. No entanto, também se entende, à semelhança do que sucede noutros ordenamentos jurídicos, que mesmo tratando-se de pesquisas prolongadas no tempo, o prazo de utilização deste meio de obtenção de prova deverá ser mais curto, salientando-se que nos ordenamentos jurídicos estudados este é de um mês, prorrogável por igual período.

CONCLUSÃO

Ao longo deste trabalho procurou-se refletir sobre o impacto dos avanços tecnológicos na atividade de investigação criminal, quer do ponto de vista dos infratores, que cada vez mais se socorrem de medidas anti-forenses, quer das Polícias, que alicerçadas na Ciência Forense Digital poderão beneficiar de soluções inovadoras e eficazes.

Atualmente é indiscutível a importância dos meios de obtenção de prova em ambiente digital, consagrados na Lei do Cibercrime, tendo-se salientado que, no essencial, estes assumem um caráter transversal na investigação criminal, não se limitando aos crimes cometidos por meio de um sistema informático.

No que concerne à pesquisa de dados informáticos, constatou-se que o seu fundamento assenta "na modernização e harmonização das legislações nacionais relativamente à busca e apreensão de dados informatizados armazenados", no âmbito da investigação criminal, como se salienta no ponto 184 do Relatório Explicativo da Convenção do Cibercrime.

Acerca do seu âmbito, salientou-se que os dados poderão estar armazenados em computadores, *tablets, smartphones* e em diversos suportes de armazenamento de dados, bem como na *cloud*, não se podendo ignorar esta realidade que assume cada vez mais importância.

Destacou-se ainda a inovação introduzida pela norma prevista no art.º 15.º, n.º 5, que consagra uma competência territorial irrestrita às autoridades nacionais no que respeita à pesquisa e apreensão remota de dados em sistemas informáticos armazenados em território estrangeiro, radicando a mesma em razões de eficácia na recolha de prova digital. No entanto, nos termos do art.º 25.º, esta possibilidade está vedada às autoridades estrangeiras.

Refletiu-se ainda acerca da necessidade de incluir novos recursos tecnológicos nos meios de obtenção de prova previstos que possam, de forma eficiente, garantir a recolha de prova digital, ultrapassando-se assim os entraves criados por diversas soluções tecnológicas que, entretanto, se vulgarizaram e que podem ser utilizadas para inviabilizar as diligências de investigação.

Destacou-se a utilização do *malware* que pode ser especificamente adaptado a pesquisas de dados informáticos, que seriam realizadas remotamente, sem o conhecimento do visado e com capacidade para obter elementos suscetíveis de valer como prova. Esta solução encontra-se consagrada, nomeadamente, na Alemanha, Espanha e França.

As possibilidades que a atual tecnologia oferece são vastas e evoluem diariamente. As ameaças potenciadas por este progresso exigem uma adaptação necessária e urgente das normas processuais penais a esta realidade. No entanto, não se pode olvidar que a consagração de novos meios de obtenção de prova em ambiente digital, ocultos ao visado, que se venham a afigurar como essenciais à atividade de investigação criminal, terá que resultar sempre, do que foi exposto ao longo da presente dissertação, de uma lei expressa anterior e suficientemente detalhada, em consonância com o princípio da legalidade.

No que tange à sua utilização, defendeu-se que a pesquisa de dados remota, sem o conhecimento do visado, é um meio de obtenção de prova especialmente restritivo dos direitos dos cidadãos, inadmissível à luz do atual ordenamento jurídico português.

De iure condendo, atendendo, desde logo, à necessidade de se consagrarem meios eficazes no combate a uma criminalidade cada vez mais sofisticada, urge proceder à alteração da lei do cibercrime, prevendo-se de forma clara e detalhada a pesquisa de dados informáticos de forma remota e sem o conhecimento do visado, através de meios informáticos adequados, em consonância com os princípios e valores jurídico-constitucionais e com a jurisprudência já consolidada do TEDH.

Este meio de obtenção de prova deverá ser utilizado no âmbito de um catálogo de crimes que englobe, designadamente a criminalidade especialmente violenta e organizada, devendo a sua autorização estar na esfera de atuação do JIC, a quem caberá a decisão de ponderar face aos interesses jurídicos em causa qual deverá ser sacrificado, sendo certo que essa ponderação terá sempre que implicar o respeito pelos princípios constitucionais que estruturam o nosso Estado de Direito democrático.

BIBLIOGRAFIA

Albuquerque, P. P. (2008). *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem.* Lisboa: Universidade Católica Editora.

Albuquerque, P. P. (2011). *Comentário ao Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem.* Lisboa: Universidade Católica.

Antunes, M., & Rodrigues, B. (2018). *Introdução à cibersegurança: A internet, os aspetos legais e a análise digital forense.* Lisboa: FCA - Editora de Informática.

Batista, L. J. (2018). *O malware como meio de obtenção de prova em processo penal (Dissertação de Mestrado).* Lisboa. Obtido de https://repositorio.ul.pt/bitstream/10451/37574/1/ulfd137535_tese.pdf

Bravo, R. (2006). *Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta*. *Revista Polícia e Justiça*.

Braz, J. (2009). *Investigação criminal: a organização, o método e a prova. Os desafios da nova criminalidade.* Coimbra: Edições Almedina, S.A.

Brenner, S. (2011). Brenner, Susan W., Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force. . *Mississippi Law Journal, 81*. Obtido em 1 de novembro de 2020, de SSRN: https://ssrn.com/abstract=1950703

Brito, M. B. (2018). *Novas tecnologias e legalidade da prova em processo penal.* Coimbra: Almedina.

Canotilho, J. G., & Moreira, V. (2007). *Constituição da República Portuguesa anotada* (4ª ed., Vol. I). Coimbra: Coimbra Editora.

Cardoso, R. (2019). *A apreensão de mensagens de correio eletrónico e de natureza semelhante*. (CEJ, Ed.) *Direito Probatório, Substantivo e Processo Penal*, 63-122.

Chynoweth, P., & Gomes, J. C. (2010). *Investigação jurídica: Uma perspetiva anglo-saxónica*. *Lusíada.Direito.Porto*, pp. 185-199.

Conde Correia. (2014). *Prova digital: as leis que temos e a lei que devíamos ter.* (Vol. 139). RMP.

Costa Andrade, M. (2013). *Sobre as proibições de prova em processo penal.* Coimbra: Coimbra Editora.

Coutinho, C. P. (2014). *Metodologia de investigação em ciências sociais e humanas: Teoria e prática.* Coimbra: Almedina.

Cybercrime Division. (2014). *Eletronic Evidence Guide - A basic guide for police officers, prosecuters and judges.* Estrasburgo: Conselho da Europa. Obtido em 03 de abril de 2020, de https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4

Cunha, P. F. (2018). *Filosofia do Direito - Fundamentos, Metodologia e Teoria Geral do Direito.* Coimbra: Almedina.

Dá Mesquita, P. (2010). *Processo penal, prova e sistema judiciário.* Coimbra: Coimbra Editora.

Deshaies, B. (1992). *Metodologia da investigação em ciências humanas.* Lisboa: Instituto Piaget.

Directorate General For Internal Policies. (2017). *Legal Frameworks for hacking by law enforcement: identification, evaluation and comparision of Practices.* European Parliament. Obtido em 1 de novembro de 2020, de https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

Elias, L. (2018). *Ciências policiais e segurança interna: Desafios e prospetiva.* Lisboa: ISCPSI - ICPOL.

Fernandes, V. (2018). *A necessidade de desencriptação de smartphones para obtenção de prova no processo penal: restrições ao princípio da não-incriminação na era digital(Tese de mestrado).* Obtido de http://repositorio.ul.pt/bitstream/10451/33972/1/ulfd135247_tese.pdf

Garfinkel, S. (2010). *Digital forensics research: the next 10 years. Digital Investigation*, 64-73. Obtido em 13 de setembro de 2020, de https://www.sciencedirect.com/science/article/pii/S1742287610000368

Gouveia, J. B. (2020). *Direito da Segurança - Cidadania, Soberania e Cosmopolitismo.* Coimbra: Almedina.

Jansen, W., Ayers, R., & Brothers, S. (2014). *Guidelines on mobile device forensics.* National Institute of Standars and Technology. Obtido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incidente response.* NIST. Obtido em 01 de setembro de 2020, de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Kerr, O. (2005). *Digital evidence and the new criminal procedure* (Vol. 105). Columbia Law Review. Obtido de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=594101

Larenz, K. (1997). *Metodologia da Ciência do Direito.* Lisboa: Fundação Calouste Gulbenkian.

Lewis, J. A., Zheng, D. E., & Carter, W. A. (2017). *The effect of encryption on lawful access to communications and data*. *CSIS - Center for strategic international studies*. Obtido em 19 de setembro de 2020, de https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf

Marcolino de Jesus, F. (2019). *Os meios de obtenção de prova em processo penal.* Coimbra: Almedina.

Mendes, P. S. (2013). *Lições de direito processual penal.* Coimbra: Almedina.

Natário, R. (2013). *O combate ao cibercrime: Anarquia e ordem no ciberespaço*. *Revista Militar n.º 2541*. Obtido em 25 de abril de 2020, de https://www.revistamilitar.pt/artigo/854

Neves, R. C. (2011). *As ingerências nas comunicações eletrónicas em processo penal.* Coimbra: Coimbra Editora.

Nunes, D. A. (2019). *O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada.* Coimbra: GESTLEGAL.

Nunes, D. R. (2018). *Algumas reflexões em matéria de apreensão de correio eletrónico e registos de comunicação de natureza semelhante*. *Cyberlaw by CIJIC*, 10-36.

Nunes, D. R. (2018). *Os meios de obtenção de prova previstos na lei do cibercrime.* Coimbra: GESTLEGAL.

Nunes, D. R. (2019). *Sobre a admissibilidade da obtenção de dados de localização através de sistema GPS à luz do Direito Português e do Acórdão Ben Faiza c. França do Tribunal Europeu dos Direitos do Homem.* Julgar Online. Obtido em 17 de novembro de 2020, de http://julgar.pt/sobre-a-admissibilidade-da-obtencao-de-dos-dados-de-localizacao-atraves-de-sistema-gps-a-luz-do-direito-portugues-e-do-acordao-ben-faiza-c-franca-do-tribunal-europeu-dos-direitos-do-homem/

Nunes, D. R. (2020). *Da admissibilidade da utilização de benware no Direito Português*. *Cyberlaw by CIJIC*, 10-58. Obtido em 17 de novembro de 2020, de https://www.cijic.org/wp-content/uploads/2020/10/3_Da-admissibilidade-da-utilizacao-de-benware-no-direito-portugues.pdf

Palma, F. (2018). *Direito penal - Conceito material de crime, princípios e fundamentos. Teoria da Lei penal: interpretação, aplicação no tempo, no espaço e quanto às pessoas.* Lisboa: AAFDL.

Pereira, R. S. (2019). *O acesso (unilateral e sem recurso a mecanismos de cooperação judiciária internacional) a dados armazenados em sistemas informáticos localizados no estrangeiro*. *Revista de Estudios Europeos*, 246-273. Obtido de http://www.ree-uva.es/index.php/sumarios/2019/n-extraordinario-monografico-1-2019/164-o-acesso-unilateral-e-sem-recurso-a-mecanismos-de-cooperacao-judiciaria-internacional-a-dados-armazenados-em-sistemas-informaticos-localizados-no-estrangeiro.

Pica dos Santos, N. R. (X-XI-XII - 2013-2014-2015). *Regime jurídico do correio eletrónico: dos momentos do correio eletrónico...à consagração de uma proteção jurídica uniforme pela Lei do Cibercrime*. *POLITEIA - Revista do Instituto de Ciências Policiais e Segurança Interna*, 235-262.

Poças, L. (2020). *Manual de investigação em direito - metodologia da preparação de teses e artigos jurídicos.* Coimbra: Almedina.

Poiares, N. C. (2019). A cibersegurança à luz da criminologia moderna. *Cyberlaw*. Obtido de https://www.cijic.org/wp-content/uploads/2019/05/Nuno-Poiares_A-CIBERSEGURAN%C3%87A-%C3%80-LUZ-DA-CRIMINOLOGIA-MODERNA.pdf

Quinlan, S., & Wilson, A. (2016). *A brief history of law enforcement hacking in the United States.* New America. Obtido em 20 de setembro de 2020, de https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf

Quivy, R., & Campenhoudt, V. L. (2005). *Manual de investigação em ciências sociais.* Lisboa: Gradiva.

Ramalho, D. S. (2013). *A investigação criminal na Dark Web*. *Revista de Concorrência e Regulação IV, n.º 14-15*, 383-429.

Ramalho, D. S. (outubro-dezembro de 2013). *O uso de malware como meio de obtenção de prova*. *Revista da concorrência e regulação*, 195-243.

Ramalho, D. S. (2014). *A recolha de prova penal em sistemas de computação em nuvem*. *Revista de Direito Intelectual, N.º 2*.

Ramalho, D. S. (2017). *Métodos ocultos de investigação criminal em ambiente digital.* Coimbra: Almedina.

Ramos, A. D. (2013). *Do periculum in mora da atuação da autoridade judiciária ao fumus boni iuris da intervenção policial.* Sintra: Comunicação apresentada no IV Congresso de Processo Penal - Congresso Luso-Brasileiro sobre Criminalidade Económico-financeira (Grupo Almedina), que teve lugar no Hotel Altis, em Lisboa, nos dias 11 e 12 de Abril de 2013.

Ramos, A. D. (2014). *A prova digital em processo penal: O correio eletrónico.* Lisboa: Chiado Editora.

Ramos, A. D. (2015). *A prova digital na investigação do (ciber)terrorismo*. *Investigação criminal n.º 9*, 110-135.

Rodrigues, B. S. (2011). *Da prova penal tomo IV - Da prova eletrónico-digital e da criminalidade informático-digital.*

Sammons, J. (2014). *The basics of digital forensics: the primer for getting started in digital forensics.* Waltham: Syngress.

Santos, P., Bessa, R., & Pimentel, C. (2008). *Cyberwar - O fenómeno, as tecnologias e os actores.* Lisboa: FCA - Editora de Informática, Lda.

Silva, G. M. (2000). *Curso de Processo Penal I.* Lisboa: Editorial Verbo.

Vacca, J. R. (2005). *Computer Forensics: Computer Crime Scene Investigation, Second Edition.* Boston, Massachussets: Charles River Media.

Valente, M. M. (2020). *Cadeia da custódia da prova.* Coimbra: Almedina.

Valente, M. M. (2020). *Direito Penal do Inimigo e o Terrorismo .* Coimbra: Almedina.

Venâncio, P. D. (2006). *Investigação e meios de prova na criminalidade informática.* Verbo Jurídico. Obtido de https://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf

Venâncio, P. D. (2011). *Lei do cibercrime - anotada e comentada.* Coimbra: Coimbra Editora.

Verdelho, P. (2004). *A obtenção de prova no ambiente digital* (Vols. A.25, N.99 (Jul./Set.2004)). Lisboa: Revista do Ministério Público.

Verdelho, P. (2009). *A nova lei do cibercrime* (Vols. Tomo LVIII n.º 320 (Outubro-Dezembro. 2009)). Braga: SCIENTIA IURIDICA.

Verdelho, P. (2015). *Lei do Cibercrime, em AA. VV., Enciclopédia de Direito e Segurança (coord. Jorge Bacelar Gouveia e Sofia Santos).* Coimbra: Almedina.

Verdelho, P., Bravo, R., & Rocha, M. L. (2003). *Leis do cibercrime - Volume I.* Famalicão: Edições Centro Atlântico.

Winter, L. B. (2017). *Registro Remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015*. *Boletín del Ministerio de Justicia*. Obtido em 16 de novembro de 2020, de https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428206148?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filename%3D1701_Estudio.pdf&blobheadervalue2=1288794492107

JURISPRUDÊNCIA

Acórdão do TC 155/2007, de 02/03/2007, acessível em: http://www.tribunalconstitucional.pt/tc/acordaos/20070155.html

Acórdão do TC 126/2013, de 27/02/2013, acessível em: http://www.tribunalconstitucional.pt/tc/acordaos/20130126.html

Acórdão do TC 340/2013, de 17/06/2013, acessível em: http://www.tribunalconstitucional.pt/tc/acordaos/20130340.html

Acórdão do TEDH, de 02/08/1984 (caso Malone c. Reino Unido), acessível em: https://hudoc.echr.coe.int/

Acórdão do TEDH, de 17/12/1996 (caso Sauders c. Reino Unido), acessível em: https://hudoc.echr.coe.int/

Acórdão do TEDH, de 11/07/2006 (caso Jalloh c. Alemanha) acessível em: https://hudoc.echr.coe.int/

Acórdão do TEDH, de 02/09/2010 (caso Uzun c. Alemanha) acessível em: https://hudoc.echr.coe.int/

Acórdão do TEDH, de 08/02/2018 (caso Bem Faiza c. França) acessível em: https://hudoc.echr.coe.int/

Acórdão do TRL de 19/06/2014, acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/eb1460fa14510bf380257d080036a9b9?OpenDocument

Acórdão do TRE, de 20/01/2015, acessível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument

Acórdão do TRP, de 05/04/2017, acessível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/16ebc99e65fc19038025810c0051991a?OpenDocument

Acórdão do TRL, de 06/02/2018, acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument

Acórdão do TRL, de 07/03/2018, acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a411de057cfd2e1d80258507004c7e4e?OpenDocument

Acórdão do TRL, de 22/01/2019 acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/09b85b00ee0cc22780258397003622cc?OpenDocument&Highlight=0,consentimento,obrigatoriedade,de,defensor

Acórdão do TRL, de 04/02/2020, acessível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument