UNIVERSIDADE D
COIMBRA

José Ricardo Marques Branco

PROVA DIGITAL

OS MEIOS DE OBTENÇÃO DE PROVA DIGITAL E A RESTRIÇÃO DE DIREITOS DO ARGUIDO

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses orientada pela Professora Doutora Sónia Mariza Florêncio Fidalgo, apresentada à Faculdade de Direito da Universidade de Coimbra.

Fevereiro de 2021

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

José Ricardo Marques Branco

PROVA DIGITAL

OS MEIOS DE OBTENÇÃO DE PROVA DIGITAL E A RESTRIÇÃO DE DIREITOS DO ARGUIDO

Digital Evidence

The Means of Obtaining Digital Evidence and the Restriction of Rights of the Defendant

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Ciências Jurídico-Forenses (conducente ao grau de Mestre)

Orientadora: Prof. Dra. Sónia Mariza Florêncio Fidalgo

Coimbra, 2021

AGRADECIMENTOS

À Faculdade de Direito da Universidade de Coimbra, instituição que contribuiu decisivamente para a minha formação, quer académica quer pessoal.

À Senhora Professora Doutora Sónia Mariza Florêncio Fidalgo, minha orientadora, pela sua generosa solicitude e sábia orientação, apesar de todos os constrangimentos que a pandemia causou.

Aos meus amigos, por sempre me terem apoiado e incentivado.

À Matilde, por todo o amor, carinho, e por toda a paciência.

À minha família, por tudo o que fizeram por mim.

E em especial,
Ao meu pai, por todos os ensinamentos,
À minha mãe, por toda a força,
Por todo o amor, esforço, dedicação, e apoio incondicional.
Sem vós, não seria possível.

Obrigado!

RESUMO

O mundo atual está altamente marcado pela tecnologia, e por relevantes avanços informático-digitais que a têm caraterizado. O fenómeno que se tornou a Internet, revolucionou a sociedade de tal forma que esta pode ser considerada um dos principais pontos de referência instrumental de qualquer atividade. Todas as áreas fazem uso das suas potencialidades e, como não poderia deixar de ser, o Direito, como regulador da sociedade não fica indiferente às capacidades das ferramentas informáticas.

Contudo, também pela sua dinâmica, nem tudo o que ela comporta é positivo, o que motivou que o Direito tivesse de adaptar-se a esta nova realidade. O surgimento da prova digital e de legislação que a regulasse foi a chave para o início do combate à criminalidade informática.

No nosso ordenamento jurídico, foi dado um grande salto no que diz respeito a esta matéria com a Lei n.º 109/2009, de 15 de Setembro, à qual se deu o nome de Lei do Cibercrime. Trouxe para o ordenamento medidas de cooperação internacional, também alargou o leque da tipificação dos crimes informáticos, e veio inserir os chamados meios de obtenção de prova digital. Quanto a estes últimos a sua utilidade é inegável, são uma ferramenta poderosa no combate ao cibercrime. Mas, devido às suas características, como por exemplo, invasão da esfera da vida privada das pessoas, há o risco de poderem ofender ou pôr em causa direitos fundamentais, constitucionalmente plasmados.

O arguido, embora não seja o único, é um dos principais alvos destas medidas de obtenção de prova digital, pelo que importa saber se a sua posição fica, de certa forma, fragilizada no âmbito do processo penal.

PALAVRAS CHAVE

Prova Digital, Lei Do Cibercrime, Meios de Obtenção de Prova Digital, Direitos Fundamentais, Arguido.

ABSTRATC

Today's world is highly marked by technology, and by relevant computer-digital advances that characterize it. The phenomenon that has become the Internet has revolutionized society in such a way that it can be considered one of the main instrumental points of reference for any activity. All areas make use of their potential, and as it could not be otherwise, Law, as the regulator of society, is not indifferent to the capabilities of computer tools.

However, and also due to its dynamics, not everything that it contains is positive, which motivated the Law to have to adapt to this new reality. The emergence of digital evidence and the legislation that regulates it is the key to the beginning of the fight against cybercrime.

In our legal system, a great leap has been made with regard to this matter with the Law No. 109/2009, of 15 September, which has been called the Cybercrime Law. It brought international cooperation measures to the planning, it also extended the range of typification of computer crimes, and came to insert the so-called means of obtaining digital evidence. As for the latter, their usefulness is undeniable, they are a powerful tool in the fight against cybercrime. However, due to their characteristics, such as, for example, invasion of the sphere of people's private life, there is a risk that they may offend or undermine fundamental rights, present on the constitution.

The defendant, although he is not the only one, is one of the main targets of these measures to obtain digital evidence, so it is important to know if his position is, in a way, weakened in the context of criminal proceedings.

KEYWORDS

Digital Evidence, Cybercrime Law, Means of Obtaining Digital Evidence, Fundamental Rights, Defendant.

LISTA DE SIGLAS E ABREVIATURAS

Ac. – Acórdão

Al. – Alínea

Art. – Artigo

C. Civil – Código Civil

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CEDH – Convenção Europeia dos Direitos do Homem

Cfr. – Conforme

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

IP – Internet Protocol

LC – Lei do Cibercrime

MP – Ministério Público

N.º – Número

NTIC – Novas Tecnologias de Informação e Comunicação

OPC – Órgãos de Polícia Criminal

PGR – Procuradoria Geral da República

P. – Página

PP. – Páginas

RGIT – Regime Geral das Infrações Tributárias

RJAE – Regime Jurídico das Ações Encobertas

SS. – Seguintes

STJ – Supremo Tribunal de Justiça

Vol. – Volume

ÍNDICE

I – INTRODUÇÃO

A sociedade atual sofre alterações constantes, que se fazem sentir com maior relevo nas áreas mais preponderantes do Estado. Ao longo dos últimos anos temos visto grandes avanços tecnológico-informáticos, o que, sem ser necessária uma exaustiva pesquisa, podemos dizer que vieram facilitar o dia-a-dia do cidadão comum. Atualmente, uma transferência bancária, compras de qualquer tipo, comunicações, uma simples investigação, entre outros, estão apenas à distância de um "clique". PEDRO DIAS VENÂNCIO assinala que o impacto da Informática na nossa sociedade é tao grande que se constitui meio exclusivo que possibilita a ocorrência de determinadas relações económicas, sociais e culturais à distância, que de outro modo não existiriam[1].

Podemos assim dizer, sem qualquer problema, que esta evolução tremenda das NTIC, nomeadamente o crescimento e o aumento do uso da Internet, vieram facilitar a comunicação e o modo de vida das pessoas.

Mas, como nem tudo são benefícios, as NTIC também vieram a revelar aspetos negativos. Verifica-se um desfasamento entre a velocidade da evolução dos meios informáticos e a necessária resposta reguladora do direito.

Sendo a internet um espaço virtual, imaterial, serve também como meio para a prática de crimes, o Cibercrime. Crimes esses que podem ser informáticos, que surgiram da evolução tecnológica, ou não informáticos, crimes que já existiam, mas que aqui ganham outra forma de execução. Seguindo a linha de PEDRO DIAS VENÂNCIO podemos afirmar que a criminalidade informática não se restringe aos crimes em formato digital, mas também a qualquer tipo de crime praticado por meio informático, mesmo apenas como instrumento[2].

Com o crescimento deste tipo de criminalidade, os países tiveram de adaptar a sua legislação à nova realidade. Em Portugal, o legislador deu início a este combate com a Lei n.º 109/91, de 17 de Agosto. A grande lacuna desta lei residia na falta de um regime jurídico de recolha de prova digital, tornando-se deficitária. Foi revogada dando lugar à lei que hoje ainda nos regula nesta matéria, a Lei do Cibercrime n.º 109/2009, de 15 de Setembro. Além

[1] VENÂNCIO, Pedro Dias, *Lei do Cibercrime: Anotada e Comentada*, Coimbra Editora, 2011, pp. 14 – 15.
[2] "*as tecnologias da informação e da comunicação podem ser utilizadas enquanto instrumentos (muitas vezes mais eficazes quer nos danos causados quer no encobrimento da identidade dos seus autores) para a prática de crimes usuais da realidade corpórea e cujo tipo legal está previsto sem considerar a utilização dos meios tecnológicos como um elemento integrador do crime*" *In* VENÂNCIO, Pedro Dias, *Lei do Cibercrime: Anotada e Comentada*, Coimbra Editora, 2011, pp. 17 – 18.

desta, destacamos ainda a Lei n.º 32/2008, de 17 de Julho, e o Código de Processo Penal. Encontramos assim no nosso ordenamento, (além dos tradicionais meios de obtenção de prova), os Meios de Obtenção de Prova Digital, que consideramos uma ferramenta altamente eficaz no combate à criminalidade informática, pois esta "*representa um caminho de soluções, que mais que nunca necessita de ser percorrido*"[3].

A presente dissertação tem por objetivo tratar do tema da Prova Digital em Portugal, fazendo uma análise dos Meios de Obtenção de Prova Digital, bem como analisar o próprio regime legal da Prova Digital, apresentando os seus principais problemas, recorrendo a doutrina e jurisprudência portuguesas na investigação.

Quer os Meios de Obtenção de Prova Digital, quer a própria utilização da Prova Digital podem resvalar e atacar Direitos Fundamentais[4], pois ao tentarmos apurar a verdade material ao longo da investigação penal, usando a Prova Digital, corremos o risco de pôr em causa Direitos, Liberdades e Garantias consagrados na CRP. Aqui, e como não pode deixar de ser, importa ressalvar em que posição fica o sujeito sobre o qual recai o processo penal, o arguido. Devemos analisar até que ponto os seus direitos estão restringidos, e ver também se este está obrigado a colaborar na aplicação destas medidas ou se, por outro lado, se encontra protegido pelo princípio da não autoincriminação.

1. A Prova no Processo Penal Português. Breve Contextualização.

Ao dar início a este estudo, entendemos que é importante contextualizar o panorama processual penal do nosso país, e também, para melhor compreensão do tema central, aludir ao conceito da prova tradicional no processo penal português. Assim, faz todo o sentido que no primeiro ponto desta dissertação, a natureza do processo penal português e os princípios que regulam a prova, sejam referenciados.

O Direito Processual Penal "*faz parte integrante da denominada «ciência total do direito penal», onde se integra o direito penal em sentido amplo, a criminologia e a política*

[3] ALMEIDA, Ivo Filipe de, *A Prova Digital*, Librum Editora, 2018, p. 15.

[4] "*os já mencionados novos meios de comunicação, se permitiriam que esta se realizasse com enorme facilidade, alcançando um variado número de pessoas com uma rapidez estonteante, resultaram também em formas mais susceptíveis de intromissões não desejadas de terceiros*.", *In* NEVES, Rita Castanheira, *As Ingerências nas comunicações eletrónicas em processo penal natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prov*a, Coimbra Editora, 2011, p. 24.

criminal. É no direito penal em sentido amplo que, a par do direito penal substantivo e do direito da execução de penas e medidas de segurança, se localiza o direito processual penal"[5].

Com isto, não queremos dizer que o direito processual penal tem um carácter instrumental face ao direito penal, nem se confundem. Nas palavras de FIGUEIREDO DIAS podemos dizer que entre ambos há uma "*relação mútua de complementaridade funcional que, só ela, permite também concebê-los como participantes de uma mesma unidade*"[6]. Esta *relação mútua de complementaridade funcional* está bem assente em institutos como a *queixa* (Art.s 113º a 116º do CP e 49º e 51º do CPP) e a *acusação particular* (Art.s 117º do CP, 50º e 51º do CPP), relativamente aos quais é atribuída natureza diferente, quer seja jurídico-processual, quer jurídico-substantiva, quer mesmo de natureza dupla[7].

O processo penal português cumpre três finalidades: a *realização da justiça e descoberta da verdade material*, a *proteção perante o Estado dos direitos fundamentais das pessoas*, e o *restabelecimento da paz jurídica*[8]. Como mais à frente vamos analisar, estas finalidades podem entrar em conflito, não sendo integralmente harmonizáveis. Para FIGUEIREDO DIAS, a via de superação desta *não harmonização integral* das finalidades do direito processual penal deve passar por "*operar a concordância prática das finalidades em conflito; de modo a que de cada uma se salve, em cada situação o máximo de conteúdo possível, otimizando os ganhos e minimizando as perdas axiológicas e funcionais*", tendo sempre como limite o princípio da dignidade da pessoa humana[9].

No que diz respeito à estrutura do direito processual penal português, podemos assumir que tem vincado um modelo acusatório (Art. 32º, nº 5 da CRP). Identificamos aqui o chamado *princípio de acusação*, segundo o qual a entidade que julga e a entidade que investiga, são diferentes, o MP investiga e o Juiz julga. Neste modelo FIGUEIREDO DIAS[10] ainda acrescenta um princípio subsidiário de *investigação* a cargo do juiz.

---

[5] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2017, p. 7.
[6] Cfr. DIAS, Figueiredo, *Direito Processual Penal*, Lições coligidas por Maria João Antunes, Secção de textos da Faculdade de Direito da Universidade de Coimbra, 1988-89, 5§.
[7] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2017, pp. 8 – 10.
[8] *Ibidem*, pp. 14 – 16.
[9] DIAS, Figueiredo, *O Novo Código de Processo Penal*, Textos Jurídicos – I, Ministério Público, 1987, p. 13.
[10] "*por via do poder-dever que lhe é atribuído de esclarecer e instruir autonomamente o facto sujeito a julgamento, criando ele as próprias bases necessárias à sua decisão. O tribunal pode sempre «ordenar oficiosamente a produção de todos os meios de prova cujo conhecimento se lhe afigure necessário à descoberta da verdade e à boa decisão da causa» (artigo 340º, nº 1, do CPP). Pode sempre fazê-lo em nome do carácter indisponível do objeto do processo e da intenção de prosseguir a realização da justiça e a descoberta da verdade material. Com o limite de se tratar sempre de uma prossecução processualmente valida, que garanta*

1.1. Os Princípios Reguladores da Prova

Como vimos, o processo penal português tem estrutura acusatória: quem investiga é uma entidade diferente da que julga. A investigação sob a qual nos debruçamos tem início no instituto da prova. O que é a prova? Segundo PAULO DE SOUSA MENDES, podemos afirmar que, no processo penal, a prova é "*o esforço metódico através do qual são demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou medida de segurança aplicáveis*"[11].

E o que é o ato de "provar"? Deixando de lado conceitos técnico-doutrinais referentes a este ponto, podemos apenas dizer que, provar algo em Direito é produzir um estado de certeza no julgador, tão forte, que o leva a valorar determinada situação como verdadeira.

Posto isto, e partindo do modelo acusatório acima referenciado, podemos identificar no nosso ordenamento jurídico processual penal vários princípios basilares que regulam este instituto, os quais iremos analisar de seguida.

Começamos com o chamado (1) *princípio da investigação ou da verdade material*, plasmado no artigo 340º, nº 1, do CPP, segundo o qual *o "tribunal ordena, oficiosamente ou a requerimento, a produção de todos os meios de prova cujo conhecimento se lhe afigurar necessário à descoberta da verdade e à boa decisão da causa"*. Na linha de FIGUEIREDO DIAS[12], temos aqui presente um princípio que é ao mesmo tempo um princípio geral da prossecução processual e um princípio geral da prova, e podemos também acrescentar que é o princípio segundo o qual o tribunal investiga o facto sujeito ou a sujeitar a julgamento, independentemente dos contributos da acusação e da defesa, construindo autonomamente as bases da sua decisão.

Outro relevante principio é (2) o *princípio da presunção da inocência* (Art. 32º, nº 2, da CRP, e no Art. 6º, nº 2, da CEDH, e também no Art. 48º, nº 1, da CDFUE), segundo o

a proteção dos direitos das pessoas (do arguido e de terceiros)", ANTUNES, Maria João, *Direito Processual Penal,* Almedina, 2017, p. 22.

[11] MENDES, Paulo de Sousa, «As proibições de prova no processo penal», *Jornadas de Direito Processual e Direitos Fundamentais*, Almedina, 2004, p. 132.

[12] Cfr. ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2017, pp. 163 – 164, e também DIAS, Figueiredo, *Direito Processual Penal*, Lições coligidas por Maria João Antunes, Secção de textos da Faculdade de Direito da Universidade de Coimbra, 1988-89, § pp. 164 e 195 e ss.

qual se presume inocente até ao transito em julgado da sentença de condenação, aquele sob que recai uma acusação. Assenta na ideia de que no processo penal "*têm, pois, de ser carreados todos os meios de prova necessários à demonstração da existência de crime, da punibilidade do arguido e à determinação da pena ou medida de segurança aplicáveis, ao arguido, consistindo a prova dos factos na demonstração da sua realidade em juízo (artº 341º do C. Civil)*"[13].

A prova deve conduzir à *verdade material* que o processo penal procura, sendo que essa "*há-de ser antes de tudo uma verdade judicial, prática e sobretudo, não uma verdade obtida a todo o preço mas processualmente válida*"[14]. Por outro lado, não sendo uma verdade absoluta, mas sim prática, sabemos que a prova "*também pode falhar o seu objetivo de conduzir à convicção de verdade*". Mas, também sabemos que a prova tem de ser "*sempre, plena*" e "*conduzir à convicção e não à simples admissão de maior probabilidade*", "*a prova é a demonstração da verdade dos factos juridicamente relevantes*"[15].

Para salvaguardar o princípio da investigação, e com forte ligação ao princípio da presunção da inocência, surge o (3) *princípio in dúbio pro reo* (Art. 32º, nº 2, da CRP). É o princípio segundo o qual o tribunal deve dar como provados os factos favoráveis ao arguido, quando ficar aquém da dúvida razoável, apesar da prova produzida. Por força do *princípio da investigação,* o tribunal tem o poder dever de investigar o facto sujeito a julgamento, "*independentemente dos contributos da acusação e da defesa, construindo autonomamente as bases da sua decisão, a dúvida que fique aquém da razoável deverá ser valorada de forma favorável ao arguido, tanto mais que este se presume inocente até ao trânsito em julgado da sentença de condenação*"[16].

Como se extrai do plasmado no artigo 96º do CPP, os atos processuais são praticados, em regra, de forma oral (depoimento de testemunhas, interrogatório, leitura da sentença, respeitam a forma oral). Assim, está explícito que o *(4) princípio da oralidade* no processo penal tem enorme relevância na obtenção da prova. Será correto dizer que, tendo em conta que a prioridade dos depoimentos, afirmações ou debates, são feitos oralmente, em detrimento de demais provas possíveis, nomeadamente o caso da prova documental, a

[13] JESUS, Francisco Marcolino de, *Os Meios de Obtenção da Prova em Processo Penal*, Almedina, p. 84.
[14] DIAS, Figueiredo, *Direito Processual Penal*, Coimbra Editora, 2004, p. 194.
[15] FERREIRA, Manuel Cavaleiro de, *Curso de Processual Penal*, II vol, Editora Danúbio, 1986, pp. 282 – 288.
[16] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2017, pp. 171 – 172.

produção de prova de maior relevância, é sem dúvida, a apresentada em audiência de forma oral.

No artigo 127º do CPP está consagrado o *(5) princípio da livre apreciação da prova*, segundo o qual, salvo disposição em contrário, a prova é apreciada segundo as regras da experiência e da livre convicção da entidade competente (o julgador). O princípio da livre apreciação da prova pode ser visto de forma negativa, que significa "a *ausência de critérios legais que predeterminem o valor da prova*", e de forma positiva, quando "*as entidades a quem caiba valorar a prova o façam de acordo com o dever de perseguir a realização da justiça e a descoberta da verdade material, numa apreciação que terá de ser sempre objetivável, motivável e, por conseguinte, suscetível de controlo*"[17]. Como é certo, este princípio não vale sem quaisquer limitações.

Importa ainda, por último, fazer referência ao artigo 125º do CPP, que sob epígrafe "*legalidade da prova*", diz que "*são admissíveis as provas que não forem proibidas por lei*". Encontra-se aqui consagrado o *(6) princípio da legalidade da prova*. Desta premissa, partimos para um tópico muito importante, ao qual não podemos deixar de fazer uma breve referência, as *Provas Proibidas*. O ordenamento jurídico português, na CRP e no CPP mais concretamente, contém determinadas proibições de prova.

Na CRP, partindo dos artigos 24º e 25º, tanto a vida humana como a integridade física das pessoas são consideradas invioláveis, dizendo mesmo o nº 2, do artigo 25º que "*ninguém pode ser submetido a tortura, nem a tratos ou penas cruéis, degradantes ou desumanos*". O artigo 32º, nº 8, especifica que "*são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações*". Além destes podemos também referenciar o vertido no artigo 34º, nº 1, que considera invioláveis o domicílio e a correspondência[18].

Quanto às provas proibidas no CPP, aderimos ao entendimento de FRANCISCO MARCOLINO DE JESUS[19], que parte da distinção entre:

---

[17] *Ibidem*, p. 168.

[18] No Art. 34º, nº 2 e 3, da CRP encontramos exceções a esta inviolabilidade do domicílio e correspondência. No primeiro número, a exceção à inviolabilidade "*só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei*". No segundo caso, falamos das situações em que o visado dê o seu consentimento.

[19] Cfr. JESUS, Francisco Marcolino de, *Os Meios de Obtenção de Prova*, Almedina, 2019, pp. 92 – 104.

(1) *Temas de Prova Proibidos*, que dizem respeito aos que a lei não permite que sejam investigados, onde determinados factos não podem ser objeto de prova, tal como, tudo o relacionado com o segredo de Estado (Art. 137º do CPP).

(2) *Meios de Prova Proibidos*, são aqueles que a lei não permite a sua valoração como meios de prova devido à falta de um qualquer requisito legal, não permite que de eles se faça uso.

(3) *Métodos Proibidos de Prova*, que consistem naqueles métodos que não podem ser utilizados na recolha de prova e estão previstos nos nº 1, 2 e 3 do artigo 126º do CPP.

Para terminar, falamos de uma última proibição presente no artigo 355º do CPP, sob a epigrafe "*proibição de valoração de provas*". Não são admitidas em julgamento, nomeadamente para o efeito de formação da convicção do tribunal, quaisquer provas que não tenham sido produzidas ou examinadas em audiência. No n.º 2, do mesmo artigo, está presente uma ressalva, em relação às provas contidas em atos processuais cuja leitura, visualização ou audição em audiência sejam permitidas pelos artigos 356º e 357º do CPP.

Desta forma finalizamos o ponto introdutório do nosso estudo, que consistiu na contextualização do processo penal português, na referência aos princípios da prova e às proibições legais e constitucionais, que reputamos fulcrais para a compreensão e prossecução desta dissertação.

2. A Sociedade de Informação

O ser humano está, desde o início dos tempos, em constante evolução. A forma como pensa, como se desloca, até como interage, altera-se à medida que os anos passam, com as vivências, com a experiência, moldando a sua relação consigo mesmo e com os outros, na vida em sociedade. E como já referimos anteriormente, as NTIC têm marcado o comportamento humano e a sociedade de forma impressionante. Podemos mesmo dizer, que em pleno século XXI, praticamente tudo o que nos rodeia está, direta ou indiretamente ligado a elas ou à vertiginosa dinâmica tecnológica. Os computadores, os telemóveis (agora também apelidados de *Smartphones*), os *smartwatches, tablets*, entre outros, são instrumentos relevantes e imprescindíveis na sociedade atual e estão enraizados em quase

todos os seus sectores. São relativamente raras as atividades, qualquer que seja a sua natureza, que não estejam ligadas ou dependentes da informática, e particularmente da Internet[20]. Podemos falar numa verdadeira *dependência social* das tecnologias.

Contudo, mesmo com inúmeros e relevantes benefícios que as NTIC têm trazido ao nosso quotidiano, não podemos ignorar que nem tudo é positivo. Devido à natureza do universo informático, que é impalpável, incorpóreo, podemos sem a menor dúvida dizer, que esta nova realidade levou ao surgimento de novos tipos de crime e novos modos de praticar crimes já existentes. Neste sentido FARIA COSTA[21] pronunciou-se em 1998 a favor da atuação do Direito Penal, mas, no seu entender, e reconhecendo todas as especificidades da informática, considera que se não deve autonomizar o direito informático, devendo atacar este tipo de criminalidade com os meios tradicionais do Direito Penal.

Atualmente, sabemos que o Direito Informático é uma realidade com especificidades próprias, e embora não tenha autonomia dogmática[22], o próprio legislador tem respeitado essas novas exigências que se impõem ao Direito Penal, gerando novas disposições normativas, quer a nível nacional, quer a nível internacional, como iremos ver mais à frente.

Desta forma, e na esteira de PEDRO DIAS VENÂNCIO, podemos referir que esta sociedade apelidada de "sociedade de informação", ou de comunicação, surgiu um pouco à "*margem do Direito*"[23], o que não quer dizer que esteja esquecido ou tenha sido posto de lado. Tendo em conta o carácter tão importante que os meios informáticos têm, como já referimos, devemos ter bem presente que "*o Direito irá sempre tentar alcançar um*

---

[20] Internet: "*A Internet é uma rede aberta de comunicações mundial, interligando muitos milhares de redes de computadores. Estes computadores conectam-se uns aos outros através de linhas de comunicação de altíssima velocidade, utilizando meios físicos que vão desde um par de cobre (o tradicional e conhecido fio do telefone) até rádios de microondas, fibras ópticas e canais de satélite e estão submetidos ao mesmo protocolo de comunicação - o TCP/IP. Os computadores ligados a rede permitem que suas informações estejam disponíveis à toda Internet fazendo com que cada um deles tenha ao seu dispor a possibilidade de se conectarem aos outros milhões de computadores existente na rede, de forma a poder compartilhar recursos (arquivos, programas e periféricos).*" *In* César AREAL e Tiago de AZEVEDO, Simulação de Mercados Internacionais, FEUP. - https://web.fe.up.pt/~eol/SIME/index.html (Consultado em 13/01/2021).

[21] COSTA, José Francisco de Faria, *Algumas reflexões sobre o estudo dogmático do chamado "Direito Penal Informático"*, Direito Penal da Comunicação, alguns escritos, Coimbra Editora, 1998, pp. 111 – 119.

[22] Seguimos a linha de ALEXANDRE DIAS PEREIRA, onde o Direito da Informática se apresenta como um novo ramo das ciências jurídicas caracterizado pela complementaridade e interdisciplinaridade. O autor afirma ser consensual a opinião de que o Direito da Informática não tem autonomia Dogmática e pode até contestar-se se as matérias que são objeto do seu estudo não deverão ser antes abordadas por unidades curriculares que dizem respeito. Não obstante, este autor reafirma que por vários motivos faz sentido dedicar uma unidade curricular especifica para este estudo. Cfr. PEREIRA, Alexandre Dias, *Direito da Informática, Estudo*, Vol. I, FDUC, pp. 1 – 3, disponível em https://eg.uc.pt/bitstream/10316/87707/1/Direito%20da%20Inform%C3%A1tica%20Estudos%20Vol%20I.pdf (Consultado em 10/01/2021).

[23] VENÂNCIO, Pedro Dias, *Lei Do Cibercrime: Anotada e comentada*, Coimbra Editora, 2011. p. 14.

equilíbrio harmonioso entre o combate ao cibercrime e a proteção dos direitos fundamentais de qualquer cidadão"[24].

A meu ver, e apesar de não ser extensa, a análise deste ponto, é extremamente necessária, tal como a sua individualização num capítulo próprio, pois este conceito de Sociedade de Informação[25], é o início, o "empurrão", para a continuação do presente estudo.

3. O Crime Informático.

Como já tivemos oportunidade de referir, o nosso quotidiano está marcado por vertiginosos avanços tecnológicos. Praticamente em todos os sectores da sociedade a informática é uma ferramenta fundamental e imprescindível. A internet está presente em todo o lado e é utilizada como veículo comunicacional privilegiado rápido e eficaz, desde a indústria, comércio, cultura ao lazer.

O aparecimento deste novo mundo tecnológico, desta nova realidade virtual latente à Internet, levou ao aparecimento de uma enorme panóplia de novos modos de praticar delitos, quer sejam informáticos quer o meio utilizado seja a informática[26].

Nos últimos anos verifica-se uma tendência de aumento generalizado dos delitos informáticos bastante evidente[27].

Tendo em conta o meio ou modo de agir que está inequivocamente ligado a este tipo de delitos (informáticos), levou a que lhes fosse atribuída a nomenclatura de crimes

---

[24] FREITAS, José Pedro, *Os Meios de Obtenção de Prova Digital na Investigação Criminal: O regime jurídico dos serviços de correio eletrónico e de mensagens curtas*, NOVA CAUSA, Edições Jurídicas, 2020, p. 55.

[25] RENATO LOPES MILITÃO salientou este conceito, quando referiu que "*Sobretudo a partir da década de 1980, bastas vezes acriticamente, tem sido recorrente a afirmação de que a sociedade hodierna é uma sociedade pós-industrial, da informação ou da comunicação*" *In* MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 247.
GARCIA MARQUES e LOURENÇO MARTINS identificam este conceito de "Sociedade de Informação" como aquele que "*assenta sobre o uso ótimo das novas tecnologias da informação e da comunicação, em respeito pelos princípios democráticos, da igualdade e da solidariedade, visando o reforço da economia e da prestação de serviços públicos e, a final, a melhoria da qualidade de todos os cidadãos*" *In* MARQUES, Garcia, e MARTINS, Lourenço, *Direito da Informática*, Almedina, 2006, p. 43.

[26] "*os já mencionados novos meios de comunicação, se permitiriam que esta se realizasse com enorme facilidade, alcançando um variado número de pessoas com uma rapidez estonteante, resultaram também em formas mais suscetíveis de intromissões não desejadas de terceiros*" *In* NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas em processo penal natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prov*a, Coimbra Editora, 2011, p. 24.

[27] Cfr. Relatório Anual de Segurança Interna, Ano de 2019, pp. 47 – 49, e também Relatório Anual de Segurança Interna, Ano de 2017, pp. 31 – 32.

informáticos, ou cibercrimes. Não conseguimos encontrar uma definição expressamente consagrada no nosso ordenamento jurídico para este tipo de crime, embora se deva fazer uma análise à legislação, à doutrina e à jurisprudência, para tentarmos encontrar a definição mais adequada.

O primeiro autor a referir-se a esta matéria é PEDRO VERDELHO[28], e no seu entender há três conceções de cibercrime: (1) os *crimes que recorrem a meios informáticos*, sendo apenas praticados com a possibilidade de recorrer a estes meios (previstos no CP – burla informática); (2) os *crimes que estão relacionados com a proteção de dados pessoais*, e também com a proteção da privacidade; e os (3) *crimes informáticos propriamente ditos*, que à data da sua publicação (2003), correspondiam aos tipificados na revogada Lei da Criminalidade Informática, Lei n.º 109/91, de 17 de Agosto.

Também PEDRO DIAS VENÂNCIO, nos dá uma noção de cibercrime, com duas naturezas: um (1) *conceito amplo* de cibercrime, que, nas suas palavras, consiste em "*toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios*"[29], ou seja, serão todas as atividades que podem, ou não, ser executadas com recurso a meios informáticos, sendo que estes não são necessários para a consumação. Incluem-se aqui os casos em que o meio informático não integra o tipo legal de crime, tendo em conta que esses mesmos crimes podem ser praticados com recurso a diversos instrumentos. Podemos incluir, por exemplo, os crimes de injúria, difamação, ofensas à honra.

Por outro lado, o autor refere uma aceção deste conceito em (2) *sentido estrito*, em que a cibercriminalidade é o tipo de criminalidade onde o elemento digital ou informático surge como componente que integra o tipo legal. Aqui já se recorre necessariamente a meios informáticos para a prática do crime. Incluímos nesta tipologia os crimes que estão tipificados na Lei n.º 109/2009, de 15 de Setembro (a que se dá o nome de Lei do Cibercrime, que iremos analisar posteriormente), no Código Penal e no Regime Geral das Infrações Tributárias (Por exemplo, o artigo 128º RGIT).

[28] VERDELHO, Pedro, *"Cibercrime", Direito de Sociedade da informação*, Vol. IV, APDI, Coimbra Editora, 2003, pp. 356 – 370.
[29] VENÂNCIO, Pedro Dias, *Lei do Cibercrime: Anotada e Comentada*, Coimbra Editora, 2011, p. 17.

Por último, no entender de RITA COELHO DOS SANTOS[30], também encontramos três distintas classificações, que consistem em: (1) *Crimes tipicamente informáticos*, são os que são praticados através de um computador ou um qualquer instrumento tecnológico idêntico. A existência deste instrumento informático é essencial para que esteja preenchido o tipo legal, na opinião da autora; (2) *Crimes essencialmente informáticos*, que são os crimes onde o bem jurídico violado que está em causa se traduz em algo informático, uma realidade informática, um programa informático, mas merecedor de tutela penal; e por último, temos os (3) *Crimes acidentalmente informáticos*, que são os crimes onde o computador ou objeto informático equiparado utilizado apenas serviu como um meio para os cumprir e não é condição para preencher o tipo legal[31].

Apesar destas classificações que acabámos de referir, e de se poder divergir quanto por qual optar, não podemos negar o que é evidente, que este tipo de criminalidade é uma realidade cada vez mais presente e se encontra em crescimento permanente. Do roubo de dados, da burla informática, ou a reprodução ilegítima de conteúdos que exigem alguns conhecimentos técnicos, até à injuria ou a difamação em ambiente de rede social.

O grande fator diferenciador neste tipo de criminalidade, como já fizemos referência, é o uso de instrumentos tecnológicos ou informáticos. E seguindo essa linha, segundo JOÃO CARLOS MACEDO[32], a execução dos crimes informáticos reside em três categorias: (1) *Manipulação informática*, que diz respeito a modificação ou alteração de dados; (2) *Espionagem informática*, consiste no acesso ou utilização de dados de outrem sem o seu conhecimento e contra a sua vontade; e (3) *Sabotagem informática*, que podemos caracterizar por corrupção, destruição ou qualquer outra forma de danificar dados ou sistemas informáticos.

Podemos assim anotar que na criminalidade informática, bastante complexa, torna-se muitas vezes bastante difícil identificar os infratores, por exemplo, devido à dimensão da

[30] Esta autora defende que a "*criminalidade informática faz reavivar a problemática da prova*", pois implica a existência de novos meios de prova e novos meios de obtenção de prova, SANTOS, Rita Coelho dos, *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários através da Manipulação Ilícita dos Sistemas Informáticos*, Coimbra Editora, 2005, p. 53.
[31] SANTOS, Rita Coelho dos, *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários através da Manipulação Ilícita dos Sistemas Informáticos*, Coimbra Editora, 2005, pp. 32 e ss.
[32] Cfr. MACEDO, João Carlos Cruz Barbosa de, *Direito Penal hoje: novos desafios e novas respostas*, Coimbra Editora, 2009, pp. 221 – 262 e pp. 231 – 232.

realidade virtual que é a Internet. Para muitos é simples a ocultação da sua identidade quando cometem uma infração desta natureza.

Em face da sua especificidade, há grande dificuldade em combater o cibercrime. Estas condicionantes levam alguns autores a considerar que o Direito tem dificuldade em acompanhar os desenvolvimentos informáticos podendo estar em causa a estabilidade jurídica e também a não regulação desta realidade, o que pode levar à falta de resposta do Direito tão rápida quanto a realidade o exige[33].

4. Prova Digital

4.1. Conceito

Como temos vindo a fazer referência ao longo deste estudo, o desenvolvimento tecnológico que leva à prática dos já analisados cibercrimes, trouxe uma maior facilidade na prática dos mesmos, o que, em termos genéricos, dificultou bastante a investigação das entidades competentes no que diz respeito à obtenção de prova e identificação dos autores da prática desses crimes.

Se, como já aludimos, a prática destes crimes implica uma ligação a meios tecnológicos ou informáticos, a prova que se irá recolher nestas situações também terá uma estrutura informática. Invocamos aqui o conceito de Prova Digital.

Nas palavras de BENJAMIM SILVA RODRIGUES "*a prova eletrónico-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 binaria ou digital*"[34].

Partindo do artigo 125º do CPP, onde se encontra plasmado o princípio de admissibilidade de todas as provas que a lei não proibir, fazemos referência à Prova Digital.

---

[33] Cfr. FREITAS, José Pedro, *Os Meios de Obtenção de Prova Digital na Investigação Criminal: O regime jurídico dos serviços de correio eletrónico e de mensagens curtas*, NOVA CAUSA Edições Jurídicas, 2020, p. 65.

[34] RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial*, Tomo I, Direito Penal Informático-Digital, Coimbra Editora, 2009, p. 39.

Esta, como qualquer outro tipo de prova, tem de ter valor probatório, para poder ser admitida pelo julgador. Este tipo de prova encontra-se num formato distinto, em *formato digital*, o que dificulta a sua apreensão, pois é constituída por meios técnicos específicos que exigem certos conhecimentos técnicos para a apreender e disponibilizar. O formato em causa faz com que possamos dizer que é um tipo de prova duradoura pois, não se extingue com o tempo. No que diz respeito à sua conservação pode ser armazenada e transmitida por meios de armazenamento digitais, que são já bastante habituais no nosso quotidiano (computador, *pen usb*[35], disco de armazenamento externo, entre outros.). Apesar deste formato digital, que para muitos pode ter algum descrédito porquanto pode ser eliminado com muita facilidade, ou até pode em determinadas situações ser mais fácil esconder a identidade dos seus autores, a Prova Digital tem capacidades muito amplas, pois pode abraçar inúmeros tipos de conteúdos. Quer sejam áudios, vídeos, dados de rede, programas, estes ficheiros atribuem um carácter extremamente útil e dinâmico a este tipo de prova, durante o processo e na descoberta da verdade material para a sua resolução.

Identificamos assim a Prova Digital como uma importante ferramenta no combate ao cibercrime, e apontamo-la como resposta às mais recentes necessidades que a tecnologia e a informática trazem à investigação criminal.

4.2. Características. Dificuldades e Fragilidades.

Como já tivemos oportunidade de referir, tendo em conta o contexto atual da evolução tecnológica na nossa sociedade e o consequente aumento do crime informático, a prova digital é imprescindível na investigação criminal. Esta é bastante *complexa*, e apesar de toda a sua utilidade, carrega consigo algumas fragilidades inerentes à sua estrutura.

Começamos por assinalar que estamos perante uma prova *incorpórea* (digital), *codificada*, altamente *mutável*, que exige conhecimentos técnicos especializados para poder ser investigada. Não é qualquer pessoa que consegue aceder a este tipo de dados, ou a outros

[35] Uma *Pen-USB* trata-se de um "*dispositivo de memória constituído por memória flash (EEPROM), capaz de fazer a gravação de dados com uma ligação USB tipo A, permitindo a sua conexão a uma porta USB de um computador ou outro equipamento com uma entrada USB, como um rádio ou televisão*". A velocidade de transmissão e a capacidade de armazenamento variam consoante os dispositivos, in https://pt.wikipedia.org/wiki/USB_flash_drive (Consultado em 20-12-2020).

sistemas informáticos. Tem de ser alguém que conheça técnicas especificas de investigação muito complexas e sensíveis, que não levem à perda ou alteração da prova.

Possui um carácter *temporário* e *frágil*, pois pode ser alterada ou modificada com bastante facilidade, tornando-se num tipo de prova bastante *dinâmico*, mas *instável*, o que leva a que seja necessário um cuidado redobrado do investigador na recolha da prova digital.

Partindo da ideia da fragilidade da prova digital, é importante salientar um último ponto, no qual recai grande parte da crítica: *a identificação do agente que praticou o cibercrime*. Pode ser extremamente difícil identificar[36] o concreto sujeito que praticou o crime, muitas vezes impossível. Não é fácil saber ao certo quem produziu o documento[37], utilizou o computador, o telemóvel, ou outro aparelho informático, pois não se consegue visualizar o agente[38]. Mas, no que diz respeito aos dispositivos em si já é diferente. A identificação destes é feita pelo *endereço de IP*[39]. A partir deste endereço é possível saber a localização do dispositivo que pratica determinada ato, e no caso em análise, a prática do crime informático.

Há até quem defenda que a única opção que realmente consegue identificar o agente que praticou o crime é este usar uma *assinatura digital*[40]. Este tipo de assinatura informática confere credibilidade ao documento, presumindo que quem o submeteu ou enviou tenha sido a pessoa identificada na assinatura[41]. O que está em causa é uma presunção, e não uma

---

[36] "*Refere-se que facilitam aos seus utilizadores o encobrimento das respectivas identidades e acções, bastando ter-se presente, por exemplo, que estes podem assumir identidades virtuais, tomar a identidade de terceiros (…), praticar os actos desde um computador ligado à Internet num cibercafé de qualquer parte do mundo ou simplesmente apagar a informação em escassos segundos, carregando numa tecla*", *In* MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 260.

[37] "*as NTIC facultam a alteração da data e hora, inclusive depois de os documentos serem gravados, bem como autorizam a alteração da restante informação, pelos próprios utilizadores ou por terceiros, sem deixar rasto*" *In* MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 260.

[38] "*no ciberespaço o exame da identidade e a autenticação dessa identidade não podem ser feitos visualmente, ou pela verificação de documentos ou de elementos identificadores já em si evidentes, como placas de veículos ou a aparência física, por exemplo.*" ARAS, Vladimir, *In* MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», pp. 263 – 264.

[39] Endereço de IP (Internet Protocol) – É o endereço único de cada ligação á internet. Para que os computadores possam identificar-se uns aos outros, cada ligação tem o seu próprio endereço IP na internet. É ele que permite a qualquer página da internet conhecer o fornecedor através do qual o utilizador navega e em que região habita. *In* DECO, *Internet e vida Privada, Proteja os seus dados pessoais*, Edições DECO Proteste, 2016, pp. 35 e 136.

[40] Assinatura Digital – Uma assinatura digital é um tipo específico de assinatura eletrônica que cumpre os requisitos legais mais rígidos e fornece o mais alto nível de segurança da identidade de um signatário, *in* https://acrobat.adobe.com/pt/pt/sign/digital-signatures.html (Consultado em 06/01/2021).

[41] Cfr. MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 264.

certeza[42], pois pode, por exemplo, a assinatura digital provir de local onde efetivamente ocorreu a prática do crime, mas este ter sido praticado por outrem que não o proprietário.

Por último, e seguindo o pensamento de DAVID RAMALHO[43], além de fazermos referência às características da prova digital, também é relevante saber onde pode ser encontrada, como pode ser recolhida, e no que diz respeito a esta última, deve ser feita dentro dos trâmites da Ciência Forense Digital. Esta pode ser caracterizada como "a *categoria genérica que abrange, em sentido amplo, as actividades de identificação, recolha e análise de prova digital e que inclui, entre outros ramos, a Ciência Forense Computacional*"[44]. Não existe uma opinião dominante sobre qual a metodologia correta a adotar no processo de recolha de prova digital. Encontramos modelos que se baseiam na criação de várias etapas com o objetivo de recolher a prova, mas também encontramos modelos que assentam numa recolha orientada desde o início para a demonstração de hipóteses sucessivas[45].

4.3. Os Diplomas que Regulam a Prova Digital

Após análise e estudo do panorama penal em que está circunscrita a prova digital, chega-se à conclusão de que a sua regulação se encontra circunscrita a três diplomas: o *Código de Processo Penal* (nos Art.s 187º, 188º e 189º), a *Lei n.º 32/2008*, de 17 de Julho, e por último, a *Lei n.º 109/2009*, de 15 de Setembro, a que se dá o nome de Lei do Cibercrime.

Neste contexto, em que as normas reguladoras da prova digital se encontram dispersas em vários diplomas, vemos um caminho que leva a incoerências[46] e gera

---

[42] Presunção idêntica à do Login – que consiste no processo para aceder a um sistema informático restrito, através da autenticação ou identificação do utilizador, usando credenciais previamente inseridas e registadas no sistema por esse mesmo utilizador. Essas credenciais são normalmente constituídas por um nome de utilizador (do inglês *username*) e uma palavra-passe (do inglês *password*), *In* https://pt.wikipedia.org/wiki/Login (Consultado em 29/12/2020).

[43] Cfr. RAMALHO, David da Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, 2017, pp. 108 – 146.

[44] *Ibidem*, p. 111.

[45] Neste sentido, DAVID RAMALHO faz referência ao modelo de etapas proposto pelo NIST (National Institute of Standards and Technology), que é constituído por quatro etapas na recolha da prova digital, são elas: a recolha, o exame, a análise e o relatório. Cfr. RAMALHO, David da Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, 2017, p. 130.

[46] "*Esta trilogia para além de acentuar o atual paradigma da descodificação e de negar a desejável centralidade normativa do Código de Processo Penal, contribui para a assimetria, a incoerência das soluções legais, e sobretudo, para o seu indesejável e nefasto insucesso prático" In* - CORREIA, João Conde, «Prova digital: as leis que temos e a lei que devíamos ter», Revista do Ministério Público, n.º 139, 2014, p. 30.

dificuldades práticas ao nível desta matéria, que decerto seriam resolvidas com uma intervenção legislativa que autonomizasse os diplomas. Esta autonomização facilitaria a forma como a prova digital pode ser obtida e utilizada na busca da verdade material, e também, na opinião de alguns autores, deixaria de pôr em causa a predominância do Código de Processo Penal.

Por enquanto, e ao seguir este rumo de dispersão legislativa, onde temos a prova digital disseminada em vários pontos normativos, "*o legislador anarquizou o sistema, não permitindo ao espírito e à letra de lei a melhor interpretação, complicando a sua aplicação legal*"[47].

4.3.1. O Código Processo Penal, os artigos 187º, 188º e 189º

A Lei n.º 59/98, de 25 de Agosto de 1998 não comtemplava qualquer referência à recolha ou obtenção de prova digital, estando apenas presente uma afloração no artigo 190º dessa mesma lei, abrindo as portas a uma extensão de aplicação dos três artigos anteriores "*às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, bem como a interceção das comunicações entre presentes*". Com a alteração legislativa que levou à revisão do Código de Processo Penal em 2007, este artigo 190º passou para o 189º[48] da atual lei, sendo acrescentando ao já referido, no n.º 1, "*mesmo que se encontrem guardadas em suporte digital*".

Não encontramos nestes artigos nenhum regime específico relativo à prova digital, apenas a remissão que já referimos, para os artigos 187º e 188º, que regulam as escutas telefónicas. Assim a lei atribui os mesmos requisitos e prossupostos que são exigidos na interceção de escutas telefónicas, para os meios de prova equiparados no artigo 189º do CPP.

---

[47] CANCELA, Alberto Gil Lima, *A Prova Digital: os Meios de Obtenção de Prova na Lei do Cibercrime*, Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra, sob orientação da Prof. Dra. Sónia Fidalgo, Coimbra, 2016, p. 25.

[48] COSTA ANDRADE atribui-lhe o nome de "*casa dos horrores hermenêuticos*" no sentido este andar um pouco à deriva. Possui várias realidades totalmente distintas que mereciam ser reguladas por tutelas também distintas, Cfr. ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado", a reforma do Código de Processo Penal*, Coimbra Editora, 2009, p. 185.

Neste sentido vemos que, no que concerne à prova digital, há limitações ao seu impulso. Ao ser aplicado o regime dos artigos 187º e ss., do CPP, o legislador põe em causa a prova que resulta das escutas telefónicas, e também diminui o interesse da investigação, pois limita a interceção de comunicações eletrónicas ou obtenção de dados relativos a cibercrimes, como a difamação e a injúria, por exemplo[49], isto porque no artigo 187º, n.º 1, do CPP, limita a utilização da prova digital ao catálogo aí previsto.

Assumimos assim que se fosse apenas esta norma a regular a prova digital, ficariam de fora alguns crimes informáticos, pois não preenchem os prossupostos daquele artigo (por exemplo, a al. a) do n.º 1, do 187º do CPP, que fala na ordem ou autorização destas medidas quanto a crimes com moldura penal máxima de 3 anos).

4.3.2. A Lei n.º 32/2008, de 17 de Junho

O legislador nacional, não tendo assumido a responsabilidade de incluir na revisão do Código de Processo Penal de 2007 medidas relacionadas com a prova digital, transpôs no nosso ordenamento uma Diretiva Europeia[50], que deu origem à Lei n.º 32/2008, de 17 de Junho, mantendo a lei geral, que regula normas gerais, dando origem esta lei a normas especiais.

Esta lei regula "*a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como os 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*"[51]. É imposto, no artigo 4º desta lei, aos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de rede pública de comunicações, a conservação pelo período de um ano, dos dados necessários para encontrar e identificar: (1) a *fonte* de uma comunicação, (2) o *destino* de uma comunicação, (3) a *data, hora e duração* de uma comunicação, (4) o *tipo* de

[49] ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado", a reforma do Código de Processo Penal*, Coimbra Editora, 2009, pp. 185 – 186.
[50] 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.
[51] Art. 1º, n.º 1, da Lei 32/2008, de 17 de Julho.

comunicação, (5) o *equipamento* utilizado na comunicação, e também (6) a *localização* desse equipamento.

A transmissão deste tipo de dados, partindo do disposto no Art. 9º da presente lei, depende de autorização (requerida pelo MP), por despacho fundamentado do juiz de instrução, e quando houver razões para crer que se esta é indispensável para a descoberta da verdade, ou que seria impossível de obter a prova de outra forma. Apenas podem ser alvo da informação (publicação) desses dados a figura do suspeito, o arguido, a vítima, e daquele suspeito de receber as mensagens.

4.3.3. A Lei n.º 109/2009, de 15 de Setembro

Os primeiros passos a nível normativo no combate ao crime informático no nosso país foram dados pela Lei n.º 109/91, de 17 de Agosto, a Lei da Criminalidade Informática. Com o passar do tempo esta lei foi-se tornando insuficiente, pois já não acompanhava a evolução tecnológica que o mundo vivia. Mesmo assim manteve-se em vigor durante dezoito anos, e só aí foi revogada, pela atual Lei do Cibercrime, a Lei n.º 109/2009, de 15 de Setembro.

A Lei do Cibercrime veio transpor para o nosso ordenamento jurídico a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, *relativa a ataques contra sistemas de informação*, adaptando ao direito interno a *Convenção sobre o Cibercrime do Conselho da Europa*[52]. Mais uma vez o legislador optou por elaborar um novo diploma, desta vez de aplicação geral, com disposições a nível penal material, processual e de cooperação internacional[53], em vez de proceder a alterações legislativas nesta matéria, mais concretamente no CPP, o diploma central do processo penal português. Quanto ao atraso temporal na transposição da diretiva, na opinião de COSTA ANDRADE, com esta referida

[52] A Convenção do Cibercrime do Conselho da Europa foi celebrada em Budapeste em 2001, e foi um acordo assinado entre vários Estados Membros da União Europeia e outros países (não estados-membros), com o intuito de combater a criminalidade efetuada por meios eletrónicos. Além deste, um dos principais objetivos desta convenção foi harmonizar e estreitar a relação dos países signatários implementado um sistema de cooperação internacional, onde os países se apoiam mutuamente no combate ao cibercrime. Apenas com a entrada em vigor da Lei do Cibercrime, de 2009, em Portugal foi oficialmente ratificada esta Convenção.

[53] "*Salienta-se, efectivamente, que não é possível conseguir a prova (digital) de boa parte dos crimes informáticos, e não só, sem o intercâmbio entre as entidades policiais e judiciárias dos vários países conexionados com a prática desses delitos*", *In* MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 262.

demora o legislador pecou ao ignorar as matérias de criminalidade informática durante tanto tempo, e falhou em aproximar o nosso ordenamento jurídico dos outros, que também assinaram e subscreveram a diretiva.

No que diz respeito à dispersão legislativa, concordamos com PAULO DÁ MESQUITA[54] que defende a ideia da integração destas regras no CPP, seguindo a linha do ordenamento jurídico italiano, alterando o próprio código com a inclusão de disposições processuais, adaptando assim os meios de obtenção de prova.

Podemos também acrescentar, seguindo a opinião de RENATO LOPES MILITÃO[55], que o diploma possui uma relação de complementaridade com a Lei n.º 32/2008, como podemos constatar no artigo 11º, n.º 2, da LC. Há quem entenda o contrário, como PAULO DÁ MESQUITA, que nos diz que a relação entre elas não é de todo pacifica, afirmando que a Lei do Cibercrime veio revogar o artigo 9º da Lei n.º 32/2008, uma vez que a lista de dados abrangida pela primeira é mais extensa. Embora não negue a sua importância em determinadas situações, como por exemplo "*no estabelecimento dos deveres dos fornecedores de serviços de conservação e proteção desses dados, bem como das condições técnicas operativas e destruição desses bens*"[56]. No que diz respeito à relação com o CPP, JOÃO CORREIA[57] defende que no "*ponto de vista doutrinal, parece inquestionável*" que tanto a Lei n.º 32/2008 como a Lei do Cibercrime revogaram tacitamente grande parte do regime disposto no artigo 189º do CPP.

A Lei do Cibercrime inclui um catálogo de crimes informáticos[58] no "Capitulo II". Nos artigos 3º a 8º encontramos os crimes de: *falsidade informática*, *dano relativo a programas ou a outros dados informáticos*, *sabotagem informática*, *acesso ilegítimo*, *interceção ilegítima* e *reprodução ilegítima de programa protegido*.

Além dos crimes informáticos que acabamos de referir (crimes informáticos em sentido estrito), a Lei do Cibercrime também se aplica aos crimes cometidos por meio de um

---

[54] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, p. 101.
[55] MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 275.
[56] MESQUITA, Paulo Dá, *Processo penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, p. 99.
[57] Cfr. CORREIA, João Conde, «Prova digital: as leis que temos e a lei que devíamos ter», Revista do Ministério Público, n.º 139, 2014, p. 36.
[58] No Código Penal estão presentes os crimes de *Devassa por meio de Informática no artigo 193º; Violação de correspondência ou telecomunicações no 194º;* e o de *Burla Informática no artigo 221º*. Podemos referenciar também outros, em que a sua ligação a esta matéria não é tao explicita, mas é existente: *Abuso de cartão de garantia ou crédito no artigo 225º*; *Equiparação de moeda dos cartões de garantia ou de crédito no 267º, n.º 1, al. c)*. E também, aqueles crimes em que o meio informático não é essencial, mas poderá ser um meio idóneo para a prática dos mesmos: *Ameaça (153º); Coação (154º); Difamação (180º); Injuria (181º); Ofensa a organismo, serviço ou pessoa coletiva (187º).*

sistema informático e aos quais seja necessário proceder à recolha de prova em suporte eletrónico (Art. 11º, n.º 1, al. a), b) e c) da LC).

Por último, mas não menos importante, foi implementado no nosso ordenamento jurídico, pela primeira vez, com a Lei do Cibercrime, um regime de obtenção de prova no panorama digital. Podemos acrescentar ainda, e partindo das palavras de PEDRO VENÂNCIO, com toda a evolução tecnológica que nos rodeia "*a LC apresenta-se hoje como o instrumento processual de obtenção de prova por excelência na instrução criminal, ou seja, a regra e não a exceção*"[59].

Damos assim por encerrada mais uma etapa deste estudo, passando agora para a análise das medidas processuais da Lei do Cibercrime e o início da abordagem à questão dos meios de obtenção de prova digital.

5. Os Meios de Obtenção de Prova Digital na Lei Do Cibercrime

Tal como já tivemos oportunidade de referir, com a entrada em vigor da Lei do Cibercrime, além da revisão dos tipos legais substantivos de crimes informáticos previstos na Lei n.º 109/91, de 17 de Agosto, e das medidas de cooperação internacional, veio também acrescentar novos meios de combate ao cibercrime, meios processuais, presentes na Convenção de Budapeste (já referida na nota n.º 52). Foi com a inclusão destes meios processuais que se tornou mais significativa a ratificação dessa Convenção.

Encontramos assim na Lei do Cibercrime disposições processuais de obtenção de prova em ambiente digital, destinadas a diferentes tipos de crimes. Nos artigos 12º a 17º da LC encontramos os meios de obtenção de prova relativos a preservação, revelação, injunção para apresentação, pesquisa e apreensão de dados informáticos. Estes aplicam-se aos crimes a que se refere o Art. 11º, n.º 1, da LC, são, portanto, de aplicação geral. Os artigos 18º e 19º já dizem respeito a meios de obtenção de prova de interceção de comunicações e ações encobertas. Aqui a aplicação já não é tão extensa, estando focados noutro grupo de cibercrimes.

[59] VENÂNCIO, Pedro Dias, «As medidas da prova digital da Lei do Cibercrime – regra ou exceção», Boletim da Ordem dos Advogados, n.º 123, Fevereiro de 2015, p. 41.

Vamos agora abordar os meios de obtenção de prova digital presentes nos artigos 12º a 19º da LC.

5.1. Preservação Expedita de Dados (12º da LC)

Partindo do disposto do artigo 2º, al. a) e b), onde encontramos as definições de "*dados informáticos*" e "*dados de tráfego*", podemos dizer que esta medida recai sobre "*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*" e sobre os *"dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente*".

Trata-se de uma medida cautelar, onde a autoridade judiciária ordena a preservação de dados armazenados num sistema informático, por parte dos fornecedores de serviços de comunicações, quando haja receio de que estes se possam perder, alterar, ou deixar de estar disponíveis, para assim proteger o curso da investigação e promover a descoberta da verdade material.

No que diz respeito à competência, o artigo 12º da LC não define quem é a autoridade judiciária competente. No n.º 2 atribui competência também aos OPC, desde que com prévia autorização ("*da autoridade judiciária*"). Assim, podemos assumir que a figura que se refere o n.º 1 é o MP. É importante frisar também que o n.º 2 do mesmo artigo, nos diz ainda que os OPC podem agir sem prévia autorização, quando haja urgência ou perigo na demora, devendo após tal facto, notificar o MP e transmitir-lhe o relatório previsto no artigo 253º do CPP.

A ordem de preservação de dados terá de ter presente, sob pena de nulidade: (1) a *natureza* dos dados; (2) a sua *origem* e o *destino* (se forem conhecidos); e (3) o *período* pelo qual deverão ser preservados (até um máximo de 3 meses). No entanto, o artigo não prevê

qualquer sanção quando não estiver preenchido algum destes requisitos, como por exemplo, prevê o n.º 1, do 14º da LC[60]

O n.º 4 deste artigo 12º da LC, tem expresso que quem tenha o controlo ou disponibilidade dos dados (o fornecedor de serviço), aquando da ordem de conservação, deve imediatamente preservar os dados em causa "*protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção*" (alguns autores chamam a este processo, onde os fornecedores de serviço congelam, bloqueiam, os dados, de "*quick freeze*"[61]), e fica também obrigado a assegurar a confidencialidade da aplicação da medida processual.

Apesar do seu carácter ativo na prevenção contra a eliminação ou modificação de dados, que é deveras essencial na resposta aos crimes informáticos (em sentido amplo e estrito), ou mesmo para proteção face à atuação das autoridades, a preservação expedita mostra-se pouco eficaz nos casos em que os crimes sejam praticados na Dark Web[62].

Antes de encerrar este ponto importa fazer referência ao entendimento de COSTA ANDRADE no que diz respeito à concessão de dados por fornecedores privados[63]. O autor releva o perigo que tem para a investigação criminal a "*privatização*" da mesma, com a intervenção dos fornecedores de serviços privados, no sentido em que lhes são atribuídas tarefas que podem importar sérios riscos ao nível da privacidade do utilizador.

5.2. Revelação Expedita de Dados de Tráfego (13º da LC)

De forma a garantir a preservação dos dados sobre os quais recai a medida prevista no Art. 12º da LC, o legislador diz que o fornecedor a quem tenha sido ordenada a preservação de dados, deve identificar e comunicar à autoridade judiciária ou aos OPC,

[60] Opinião seguida também por CANCELA, Alberto Gil Lima, *A Prova Digital: os Meios de Obtenção de Prova na Lei do Cibercrime*, Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra, sob orientação da Prof. Dra. Sónia Fidalgo, Coimbra, 2016, p. 34.

[61] RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova Eletrónico-Digital e da Criminalidade informático-Digital*, Rei dos Livros, 2011, p. 522.

[62] A Dark Web consiste numa parte da internet que para ser acedida é necessária a utilização de software, autorizações e configurações especificas. Insere-se na Deep Web, onde quando se acede, embora semelhante ao acesso da Internet dita normal, determinados sites estão ocultos, apenas tendo acesso quem os conhecer. Utilizada geralmente para pratica de crimes, mas não só. Cfr. RAMALHO, David, «A investigação criminal da Dark Web», *In* Revista de Concorrência e Regulação, Ano 4, n.º 14/15 (Abril – Setembro, 2013), p. 392.

[63] ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado, a Reforma do Código de Processo Penal*, Coimbra Editora, 2009, pp. 127 – 129.

assim que souber, os outros fornecedores de serviço através dos quais aquela comunicação em causa tenha sido efetuada, tendo em vista identificar todos os fornecedores de serviço e a via através da qual a comunicação foi realizada. Assinala-se aqui a importância da cooperação dos fornecedores de serviço com a autoridade judiciária competente ou os OPC.

Na esteira de BENJAMIM SILVA RODRIGUES, seguimos a ideia de que "*vigora, em matéria de divulgação expedita de dados, o princípio da suficiência, ou seja, de nada valerá a transmissão de dados cuja quantidade não seja suficiente para os efeitos de investigação criminal: (i) identificação, pela parte, dos fornecedores de serviços; e (ii) dos fornecedores de serviços; e (iii) da via pela qual a comunicação foi transmitida*"[64].

Por conseguinte, caberá à autoridade judiciária competente a determinação dos fornecedores visados, a quem ordenará que procedam à conservação e posterior revelação dos dados. Há aqui uma clara relação entre os artigos 12º e 13º da LC.

5.2.1. O parecer consultivo da PGR, do relator PAULO DÁ MESQUITA[65]

No que diz respeito a estes dois meios de obtenção de prova que acabámos de referir (5.1. e 5.2.), importa realçar o parecer consultivo n.º Convencional PGRP00003238 da PGR, que foi chamada a pronunciar-se sobre se os órgãos de polícia careciam de prévia autorização da autoridade judiciária para proceder à visualização de imagens colhidas por jornalistas, outros funcionários e pelos demais colaboradores de órgãos de comunicação. É importante esta referência, pois é relevante saber quem tem legitimidade para requerer e também para melhor compreender a preservação e revelação expedita de dados.

Neste parecer o relator PAULO DÁ MESQUITA identifica o MP como a entidade competente para dirigir o inquérito e para selecionar os atos que se destinem a investigar a existência de um crime, a determinar quem o praticou, a definir a sua responsabilidade, e

---

[64] RODRIGUES, Benjamim Silva, *Direito Penal – Parte Especial, Tomo 1, Direito Penal Informático-Digital*, 2009, p. 616.

[65] Parecer do Conselho Consultivo da PGR, com o n.º Convencional PGRP00003238, Relator: PAULO DÁ MESQUITA, 2012, disponível em: http://www.dgsi.pt/pgrp.nsf/f1cdb56ced3fdd9f802568c0004061b6/a734913d16b0f89480257af00043b68a?OpenDocument (Consultado em 18/01/2021).

também a descobrir e recolher provas "*em ordem à decisão sobre o exercício da acçao penal*".

Quanto aos OPC, e tendo em conta os fins do processo penal, estes podem realizar atividades ao abrigo da lei (medidas cautelares e de polícia, embora estando sempre dependentes de haver urgência e perigo na demora) e também por encargo do MP (onde é necessário um despacho de delegação de competência). Assim vemos que apenas podem praticar atos de investigação criminal quando houver prévio despacho de delegação de competência, que será emitido depois de ser comunicada a notícia do crime ao MP.

No caso de ser impossível comunicar com o MP competente para o caso, o OPC poderá contactar qualquer magistrado ou agente do MP, e deste receberá ordem de determinação dos atos urgentes de aquisição e conservação dos meios de prova que acharem relevantes (Art. 264º, n.º 4, do CPP). Sempre que os atos partirem de iniciativa própria do OPC, têm de estar preenchidos os prossupostos de necessidade e de urgência.

Fica assim estabelecido que as autoridades e os OPC podem, por iniciativa própria que vise a prossecução de fins do processo penal, praticar todos os atos cautelares necessários e urgentes para assegurar os meios de prova que não atinjam direitos protegidos por lei (Art. 249.º, n.º 1, do CPP), e podem também realizar os atos permitidos por previsão legal especial, dentro dos estritos pressupostos jurídico-normativos estabelecidos pela lei.

No que diz respeito à interpelação dos órgãos de comunicação social ("*jornalistas, diretores de informação, administradores ou gerentes de entidade proprietária de órgão de comunicação social ou qualquer outra pessoa que nele exerça funções*"), tendo como objetivo a solicitação de documentos ou objetos que estiverem na posse daqueles, para a prossecução de fins do processo penal, esta faz parte da competência reservada da autoridade judiciária que dirige o processo (Art. 182º, n.º 1, do CPP, Art. 135.º, n.º 1, do CPP e Art. 11.º, n.º 5, do Estatuto do Jornalista), independentemente de as imagens estarem protegidas por sigilo profissional do jornalista ou não.

Não é admissível que os OPC, por iniciativa própria, mesmo que tenham em conta a prossecução de fins do processo penal, abordem elementos de órgão de comunicação social com vista ao visionamento de imagens que estão na sua posse e foram captadas por seus colaboradores, sejam jornalistas, funcionários ou outros (Art. 182º, n.º 1, do CPP, Art. 135º, n.º 2, do CPP, Art. 11º, n.º 5, do Estatuto do Jornalista, Art. 11º, n.º 1, al. c), da LC e Art. 14.º, n.º 1 e 7, da LC). Assim, no caso em que os OPC tenham conhecimento de que estes

elementos acima referidos tenham recolhido imagens que possam ser relevantes, devem comunicar, no mais curto prazo possível, ao MP para este decidir ou promover o que achar mais conveniente.

Por último, PAULO DÁ MESQUITA fala no caso em que uma autoridade ou OPC, pode ordenar a preservação de dados a quem deles tenha disponibilidade ou controlo, se entender que tal é necessário para a descoberta da verdade no processo penal, quando haja risco de os dados recolhidos e que estejam na posse de órgão de comunicação social (seja em suporte digital ou material) se possam perder, alterar, ou deixar de estar disponíveis, estando presentes os prossupostos da urgência ou perigo da demora, e não sendo possível contactar tempestivamente o MP.

5.3. Injunção para Apresentação de Dados (14º da LC)

No artigo 14º da LC encontramos prevista a injunção para apresentação ou concessão de dados. Trata-se de um instrumento que visa permitir que a autoridade competente ordene, a quem tenha disponibilidade ou controlo desses dados, que os comunique ao processo ou que faculte o acesso a estes, sob pena de punição pela prática do crime de desobediência (Art. 348º do CP). Os dados em causa na injunção têm de estar identificados, tal como na ordem de preservação de dados (n.º 2, do Art. 14º da LC).

O n.º 4 do referido artigo alarga o seu âmbito de aplicabilidade aos fornecedores de serviço, aos quais pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes. Nesses dados deve estar incluída qualquer informação, (ainda que diferente dos dados de tráfego ou conteúdo) seja com a forma de dados informáticos ou outra qualquer, que esteja na posse do fornecedor de serviços, e que permita determinar: (1) o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; (2) a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou (3) qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

Importa assinalar a importância dos três últimos números do presente artigo. No n.º 5 está latente que a injunção não pode recair sobre o suspeito ou o arguido, estando salvaguardado aqui o princípio da não autoincriminação (*nemo tenetur se ipsum accusare*, que abordaremos mais à frente). O n.º 6 contém uma limitação ao uso da injunção excluindo do seu alcance o acesso a sistemas informáticos no exercício de atividades tais como advocacia, médica, jornalística e bancária, e também tem em conta o segredo profissional e segredo de estado, no n.º 7 (Art. 182º do CP).

5.4. Pesquisa de Dados Informáticos (15º da LC)

Este meio de obtenção de prova recai, como também vimos para o artigo 14º da LC, sobre dados informáticos que se encontram armazenados. O que se pretende concretamente é o acesso a um sistema informático, para aí proceder a uma pesquisa de dados. Não se depende aqui de um objeto físico, pois é possível aceder ao espaço digital, sem haver a chamada "intrusão no domicílio do visado".

Apesar desta característica, a esta medida é aplicado, com as necessárias adaptações, o regime de execução das buscas prevista no CPP, nos artigos 174º a 179º (o n.º 6, do Art. 15º da LC fala ainda também do regime das buscas no Estatuto do Jornalista). PAULO DÁ MESQUITA diz-nos que apesar da nomenclatura atribuída ser de pesquisa, que se trata de uma busca de dados informáticos, pois não se altera a sua natureza processual, valendo os prossupostos do artigo 174º, n.º 1 e 2, do CPP[66].

No n.º 1, do artigo 15º da LC, seguimos a linha de BENJAMIM SILVA RODRIGUES, onde diz que a interpretação desta norma deve ser feita de *forma restrita*, pois enquanto a norma demonstra que a autoridade judiciária competente deve, sempre que possível, presidir à diligencia, este autor apela a que a pesquisa não ocorra sem a presença da autoridade judiciária que a ordenou ou autorizou. Partindo da força do Art. 32º, n.º 4, da CRP o autor alega que "*esta autorização tem de ser judicial, e à semelhança do que ocorre com o 179º, n.º 3, do CPP, caberá ao juiz presidir a tal operação para que se mantenha a*

[66] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, pp. 114 – 115.

"chain of custody", ou seja, sob pena de se desconsiderar a valoração dos mesmos em virtude de não darem garantias de autenticidade, fidedignidade e não contaminação"[67].

O despacho que ordena ou autoriza esta pesquisa tem validade máxima de 30 dias (sob pena de nulidade, n.º 2, do Art. 15º, da LC).

Seguimos também o entendimento deste autor no que diz respeito ao plasmado no n.º 3. Situações em que o OPC pode proceder à pesquisa "*sem prévia autorização da autoridade judiciária, quando: a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado; b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa*.".

Apesar de no n.º 4 o legislador ter acrescentado que, quando ocorrer alguma das situações referidas acima, haverá lugar à apresentação de um relatório (nos termos do 253º CPP) à autoridade judiciária competente, e ainda no caso da al. a) ser exigida comunicação e validação por parte da autoridade judiciária competente, sob pena de nulidade, este autor tece ainda observações bastante pertinentes, às quais nos alinhamos. Quanto ao referido no ponto a), pode-se obter o consentimento de forma "engenhosa, desleal", permitindo aos OPC obter dados que não conseguiriam, sem esse mesmo consentimento.

No que à al. b) diz respeito, o autor tem uma posição mais apertada dizendo que está concretizado "*um verdadeiro direito penal do inimigo*"[68], pois neste caso o terrorista, ou criminoso violento, ou organizado, fica limitado quanto aos níveis mínimos de garantias de direitos fundamentais à luz das legítimas expectativas e garantias processuais penais que seria de esperar em virtude do plasmado no ordenamento jurídico processual penal e também constitucional português.

---

[67] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II, *Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010, pp. 446 – 447.

[68] Neste sentido, e na esteira de FIGUEIREDO DIAS, falamos de Gunther Jakobs, que idealizou a teoria do direito penal do inimigo, partindo do princípio que o "*direito penal do cidadão, aplicável a todos os que pertencem a uma «comunidade legal», não deve valer para aqueles que se recusam a participar nela, tentando obter a aniquilação dessa comunidade (os «terroristas») ou violando repetida e persistentemente as normas que os regem (os delinquentes por tendência perigosos)*" Cfr. DIAS, Jorge de Figueiredo, Direito Penal, Parte Geral, Tomo I, Questões Fundamentais, a doutrina geral do crime, Coimbra Editora, 2007, p. 36.

Este regime levado a cabo pelos OPC, com cariz excecional, será considerado prova proibida, insuscetível de valoração, quando não respeitar o estatuído nestas duas alíneas, já referenciadas do nº 4, do artigo 15º, da LC[69].

Importa por último, assinalar o disposto no n.º 5 deste artigo, que nos diz que sempre que existirem razões para crer que os dados informáticos que estão sujeitos a pesquisa se encontrem noutro sistema informático, ou em parte diferente do sistema alvo, mas acessíveis daquele ponto, a pesquisa pode ser estendida a essas situações, desde que haja autorização ou mesmo ordem da autoridade jurídica competente.

5.5. Apreensão de dados informáticos (16º da LC)

Partindo do elencado na lei, quando no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova (tendo em vista a descoberta da verdade material), a autoridade competente autoriza ou ordena a apreensão do mesmo, através de despacho devidamente fundamentado (Art. 16º, n.º 1, da LC).

Essas apreensões podem realizar-se pelos OPC, sem prévia autorização ou ordem da autoridade judiciária competente, nos termos do artigo 15º, n.º 3 e 4, quando neste caso existir perigo na demora ou urgência, desde que validadas no prazo máximo de 72 horas (n.º 2 e 4).

Quando estiverem em causa dados em que o conteúdo seja suscetível de revelar informações pessoais e íntimas, que possam pôr em causa a privacidade da pessoa visada ou de terceiro, estes deverão ser analisados por um juiz, que após ponderação, poderá ou não avançar com a sua junção aos autos, sob pena de nulidade (n.º 3).

Será relevante também, para este regime, o disposto nos n.º 5 e 6, relativos ao segredo de estado (Art. 182º do CP) e os referentes a determinadas ordens profissionais (estipulados nos seus estatutos profissionais correspondentes e também nos Art.s 180º e 181º do CPP).

Estão consagrados no n.º 7 do artigo 16º da LC, o *princípio da proporcionalidade* e o *princípio da adequação na apreensão de dados informáticos*, tendo em conta cada caso

[69] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo IV, *Da Prova Penal, Eletrónico-Digital e da Criminalidade Informático-Digital*, Rei dos Livros, 2011 p. 527.

concreto, estando elencadas as formas de atuação. Assim, pode ser apreendido o suporte onde está instalado o sistema ou o suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura. Deve ser efetuada uma cópia dos dados, em suporte autónomo, que será junta ao processo[70].

No entender de PEDRO VERDELHO, ROGÉRIO BRAVO e LOPES ROCHA, referindo-se ao artigo 19º da Convenção de Budapeste, "*com exceção da mera apreensão de dados no seu suporte, que em nada se distingue da mera apreensão, todas estas medidas (incluída apreensão de dados separadamente do seu suporte) são medidas especificas do espaço virtual. Não são por isso enquadráveis nos conceitos atuais da lei processual*"[71].

5.6. Apreensão de Correio Eletrónico e Registos de Comunicações de Natureza Semelhante (17º da LC)

O artigo 17º da LC estabelece que "*no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal*".

Esta norma aplica-se a mensagens de correio eletrónico ou a registos de comunicações de natureza semelhante, recolhidos no decurso de uma pesquisa informática, ou de outro acesso legítimo a um sistema informático. Neste sentido o acesso legitimo

---

[70] Quanto a este ponto BENJAMIM SILVA RODRIGUES afirma que em vez de duplicado a copia deveria ser feita em triplicado, Cfr. RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010, pp. 452 – 453.
ARMANDO DIAS RAMOS acrescenta ainda que se devia alterar a expressão *cópia* para *clonagem* ou *cópia de imagem*, uma vez que há ferramentas informáticas a nível forense especificas para o efeito, impedindo alterações futuras, e não se pondo em causa a discussão da valoração da prova em sede de julgamento. *In* RAMOS, Armando Dias, *A Prova Digital em Processo Penal: o Correio Eletrónico*, Chiado Editora, 2014, p. 90.

[71] VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes; *Leis do Cibercrime, Vol. 1* p. 18, excerto disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdocibercrime1.pdf (Consultado em 06/01/2021).

abriga: perícias, quando realizadas antes da apreensão, e o acesso a dados que estejam na disponibilidade ou controlo de outra entidade (Art. 14º, n.º 1, da LC)[72].

O correio eletrónico consiste no correio transmitido na internet. Quanto aos registos de comunicações semelhantes, realçamos dois grupos: as comunicações realizadas pelo número de telefone, onde podemos inserir as SMS ou MMS; e as realizadas através da internet, que englobam programas de mensagens instantâneas (Messenger, WhatsApp, Telegram, Discord)[73].

Não encontramos no artigo 17º da LC qualquer distinção entre as mensagens de correio eletrónico lidas ou não lidas[74]. Durante algum tempo o cerne da aplicação deste regime baseava-se na distinção entre correio lido e não lido, aplicando-se analogicamente ao correio eletrónico o regime da correspondência física. Assim aplicava-se ao correio eletrónico não lido o normativo aplicável à correspondência, recaindo sobre o já lido o regime geral da apreensão de documentos[75].

Esta distinção foi alvo de inúmeras discussões doutrinais, que vieram a ser resolvidas pelo artigo 17º da LC. Com a entrada em vigor[76] desta norma, o legislador demonstrou claramente a sua "*intenção de submeter toda a apreensão de correio eletrónico e registos de comunicações de natureza semelhante ao regime da apreensão da correspondência, independentemente das mensagens se encontrarem lidas ou não lidas*"[77].

No caso do correio eletrónico, e a contrário do correio físico, não há diferença em estar aberto ou fechado, ou *lido* ou *não lido*. Um e-mail ou uma mensagem equiparada podem ser abertos num dispositivo, ser "marcado como não lido" e aparecer *não lido*, mesmo depois de *lido*, com apenas um "clique". Pode também estar apresentado como *não lido* num

---

[72] Cfr. CARDOSO, Rui, «Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15/IX», Revista do Ministério Público, n.º 153, 2018, p. 179.
[73] *Ibidem*, p. 183.
[74] *Ibidem*, p. 184.
[75] RAMALHO, David, *Métodos ocultos de investigação criminal em ambiente digital*, Almedina, 2017, p. 278.
[76] "*Com a aprovação da Lei do Cibercrime, o regime de apreensão de correio eletrónico e registos de comunicações de natureza semelhante passou a estar regulado no seu Artigo 17º e, subsidiariamente (por remissão do mesmo) pelos Artigo 179º do CPP. Deixou de se aplicar a extensão legal prevista no Artigo 189º, nº 1 do CPP. Do Artigo 17º da Lei do Cibercrime resulta de forma clara que, ao contrário do que ocorre com o correio tradicional, não se distingue quanto a correio eletrónico aquele que está "aberto" do "fechado". Não há diminuição das exigências garantísticas do correio eletrónico quando aberto/lido relativamente ao correio eletrónico fechado, atenta a natureza própria destas comunicações" In* Ac. do Tribunal da Relação de Lisboa, de 07-03-2018, Processo n.º 184/12.5TELSB-B.L1-3, com relator CONCEIÇÃO GONÇALVES, disponível em www.dgsi.pt .
[77] RAMALHO, David, *Métodos ocultos de investigação criminal em ambiente digital*, Almedina, 2017, p. 278.

determinado dispositivo, e ter sido aberto e lido em outro, ao qual o destinatário acedeu (dependendo aqui das definições de sincronização de dispositivos adotadas por cada utilizador)[78].

Assim, na esteira de SÓNIA FIDALGO, podemos defender que não terá sido essa a opção do legislador pois, pela dificuldade demonstrada acima, trata-se de uma fronteira difícil de estabelecer. No seguimento do pensamento desta autora[79] entendemos também que o legislador, reconhecendo a inadequação e anacronismo da distinção, acabou por atribuir tutela acrescida à mensagem em formato digital, submetendo-a ao disposto no artigo 17º da LC, o que lhe valeu enormes criticas[80].

No que diz respeito à "*correspondente aplicação do regime de apreensão de correspondência previsto no CPP*"[81], assinalamos que este se aplica subsidiariamente (não se aplica integralmente), apenas no sentido em que não contrariar o previsto na LC. Assim , o artigo 17º da LC remete para o artigo 179º do CPP, que estabelece no seu n.º 1 que "*Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência"*.

A aplicação do regime do CPP ao correio eletrónico, no entendimento de PEDRO VERDELHO[82], deve ser feita com determinadas adaptações, a saber: (*i*) a apreensão cautelar de correio eletrónico ou mensagens equiparadas deve poder ser feita sem a autorização prévia do juiz, pois a lei não é expressa a este propósito; (*ii*) e não será necessário que o juiz seja o primeiro a ter conhecimento do conteúdo de todas as mensagens.

---

[78] FIDALGO, Sónia, «A apreensão de correio electrónico e a utilização noutro processo das mensagens apreendidas», Revista Portuguesa de Ciência Criminal, n.º 29, 2019, p. 69; E também CARDOSO, Rui, «Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15/IX», Revista do Ministério Público, n.º 153, 2018, p. 187.

[79] FIDALGO, Sónia, «A apreensão de correio electrónico e a utilização noutro processo das mensagens apreendidas», Revista Portuguesa de Ciência Criminal, n.º 29, 2019, p. 69; e também CARDOSO, Rui, «Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15/IX», Revista do Ministério Público, n.º 153, 2018, pp. 278 – 279.

[80] COSTA ANDRADE acerca destas críticas: *"(…) o legislador deve resistir à tentação e ao primeiro impulso de responder com leis – e sobretudo com leis incriminatórias – ao primeiro sinal de surpresa, de factos ou de problemas para os quais pareça não haver resposta na lei. Como de todos os lados se reconhece, a criminalização deve ser sempre o ponto de chegada de uma determinada reflexão sobre a dignidade penal e a carência de tutela penal do facto*" *In* ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado, A Reforma do Código de Processo Penal*, Coimbra Editora, 2009, p. 37

[81] Art. 17º da LC.

[82] VERDELHO, Pedro, «A nova Lei do Cibercrime», Scientia Iuridica, Tomo LVIII, n.º 320, 2009, pp. 743 – 744.

No que diz respeito ao primeiro argumento (*i*) deste autor, perfilhamos a posição de SÓNIA FIDALGO, no sentido de que apesar das dificuldades que esta problemática pode promover, a lei exige claramente, no artigo 17º da LC, a presença de despacho judicial para a apreensão de correio eletrónico[83]. A jurisprudência portuguesa também tem seguido esta posição[84].

No que concerne ao segundo argumento (*ii*) daquele autor, seguimos a opinião de RUI CARDOSO, que partindo da estrutura acusatória do processo penal português, em que a entidade que julga é distinta da que acusa, não fará muito sentido que na fase de inquérito, o juiz de instrução tome conhecimento das mensagens e proceda à seleção das que revelarem interesse para a descoberta da verdade material, visto que este deve ser o imparcial "*juiz de liberdades e garantias*"[85], não lhe devendo caber a ele a definição do objeto da acusação[86].

A jurisprudência portuguesa "*não tem sido sensível a estes argumentos*"[87] e tem defendido que a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida é o juiz de instrução criminal[88].

5.7. Interceção de Comunicações (18º da LC)

No artigo 18º da LC está prevista a interceção de comunicações eletrónicas relativas a crimes: (1) previstos na lei, ou (2) cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando esses crimes se encontrem previstos no artigo 187º do CPP.

Seguindo a linha de CRISTINA MÁXIMO DOS SANTOS, focamo-nos agora no artigo 34º, n.º 4, da CRP, onde só em processos de natureza penal é que é admissível a ingerência nas telecomunicações, cabendo à lei ordinária definir quando tem lugar, e de que

---

[83] FIDALGO, Sónia, «A apreensão de correio electrónico e a utilização noutro processo das mensagens apreendidas», Revista Portuguesa de Ciência Criminal, n.º 29, 2019, p. 67.
[84] Ac. do Tribunal da Relação de Guimarães, de 29-03-2011, Processo n.º 735/10.0GAPTL-A.G1, com relator MARIA JOSÉ NOGUEIRA, disponível em: www.dgsi.pt .
[85] CARDOSO, Rui, «Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15/IX», Revista do Ministério Público, n.º 153, 2018, p. 205.
[86] Cfr. *Ibidem*, pp. 195 – 211.
[87] FIDALGO, Sónia, «A apreensão de correio electrónico e a utilização noutro processo das mensagens apreendidas», Revista Portuguesa de Ciência Criminal, n.º 29, 2019, p. 68.
[88] Ac. do Tribunal da Relação de Lisboa, de 06-02-2018, Processo n.º 1950/17.0T9LSB-A.L1-5, com relator JOÃO CARROLA, disponível em www.dgsi.pt .

forma está limitada. Na opinião da autora "*não é em qualquer processo criminal que a ingerência para um determinado conjunto de crimes é admissível como meio de obtenção de prova, mas apenas e só para um determinado conjunto de crimes definidos por lei*"[89]. Estas interceções são as correspondentes aos crimes a que faz referência o artigo 18º, nº 1, da LC. Nos n.º 2 e 3, do mesmo artigo, encontramos plasmado que as exceções ao sigilo das comunicações devem revestir a forma de lei, e devem ser aplicadas por um Magistrado Judicial (Art. 32º, nº 4, da CRP). No caso de as provas terem sido obtidas de forma abusiva (intromissão na vida privada ou nas telecomunicações), à luz do artigo 32º, n.º 8, da CRP enferma de nulidade.

No que diz respeito à interceção e registo de transmissões de dados informáticos, segundo o n.º 4, do 18º, da LC, são aplicáveis, em tudo o que não for contrariado pelo artigo em causa, os procedimentos e autorizações judiciais previstas para as escutas telefónicas (previstas nos artigos 187º a 190º do CPP). PEDRO VENÂNCIO diz-nos que nesta situação "*falamos da interceção de mensagens de correio eletrónico em tempo real, ou seja, no seu trajeto do computador do emissor para o computador do recetor através da rede de servidores. Ou ainda a interceção de mensagens trocadas através de processos de comunicação instantânea (usualmente designados por serviços de «chat»)*"[90].

Podemos acrescentar que, estando em causa o sigilo de comunicações, quando é violado, aplica-se o artigo 384º do CP, que pune a violação do segredo de comunicações por entidade públicas. Essa restrição de estar ligada a entidades públicas está relacionada com o momento da criação da norma, pois nesse período as comunicações estavam entregues a entidades públicas, realidade bem diferente do que vivemos hoje[91]. Seja como for, aplica-se a esta matéria o artigo 194º do CP, que pune aqueles que violarem as telecomunicações ou correspondência de terceiros.

Também no Código Penal, o artigo 276º prevê a punição de quem tiver instrumento ou aparelhagem, especificamente destinados à montagem de escuta telefónica, ou à violação de telecomunicações fora das condições legais. Por outro lado, está estabelecido um regime

[89] SANTOS, Cristina Máximo dos, «As Novas Tecnologias da Informação e o Sigilo das Telecomunicações», separata da Revista do Ministério Público, n.º 99, Lisboa, 2004, p. 96.
[90] VENÂNCIO, Pedro Dias, *Lei do Cibercrime: Anotada e Comentada*, Coimbra Editora, 2011, p. 119.
[91] Cfr. RIBEIRO, Maria da Conceição Fernandes, *Cibercrime e Prova Digital*, Dissertação apresentada ao Instituto Superior Bissaya Barreto para obtenção do grau de Mestre em Ciências Jurídico-Forenses sob a orientação da Prof. Doutora Cristiane Reis e coorientação da Mestre Sara Moreira, Coimbra, 2015, pp. 66 – 67.

excecional no artigo 18º da LC, e nos artigos 187º, 188º, 189º e 190º do CPP, onde está admitida a interceção e gravação, dependente do cumprimento de determinados prossupostos. No caso de incumprimento há lugar a nulidade (Art. 190º CPP). Este regime excecional tem lugar na fase de inquérito, e apenas se houver razões para crer que tal é indispensável para a descoberta da verdade material, não havendo outra forma de obter prova. Terá de haver previamente um despacho fundamentado do juiz de instrução, mediante requerimento do MP (Art. 187º CPP).

Faz sentido quanto a este tema fazer também referência à Lei nº 41/2004, de 18 de Agosto, que regula a Proteção de Pados Pessoais e Preservação nas Telecomunicações, que no seu artigo 4º estabelece a "*Inviolabilidade das Comunicações*". No n.º 1 deste artigo temos plasmada a inviolabilidade de dados de tráfego, e no n.º 2, está proibida a interceção (por meio de escuta) ou vigilância de comunicações ou dados sem o consentimento dos utilizadores.

5.8. Ações Encobertas (19º da LC)

Em último lugar, assinalamos as ações encobertas, previstas no artigo 19º da LC. O legislador português alargou ao mundo digital as disposições sobre este tipo de ações, já previstas na Lei n.º 101/2001, de 25 de Agosto, onde está regulado o Regime Jurídico das Ações Encobertas[92].

De acordo com o n.º 1 deste artigo, as ações encobertas podem ser aplicadas, durante o inquérito, relativamente a: (1) crimes previstos na Lei do Cibercrime; a (2) crimes cometidos por meio de um sistema informático quando lhes corresponda, em abstrato, pena de prisão de máximo superior a cinco anos; a (3) crimes dolosos que, mesmo que a moldura penal seja inferior, atentem contra a liberdade e autodeterminação sexual, nos casos em que os ofendidos sejam menores, a burla qualificada, a burla informática e nas comunicações com conteúdo de discriminação racial, religiosa ou sexual, e infrações económico-financeiras; e por último, (4) crimes consagrados no Título IV do Código do Direito de Autor e dos Direitos Conexos.

[92] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II, *Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010, pp. 446 – 447.

No n.º 2 deste artigo diz-se que, no caso de haver necessidade de se recorrer a meios informáticos, se aplica o regime previsto para a interceção de comunicações.

Esta norma não se encontra isenta de críticas, pois sendo as ações encobertas um dos meios mais lesivos de obtenção de prova, não se compreende como o catálogo de crimes foi ampliado e é tao abrangente. PAULO DÁ MESQUITA pronunciou-se e critica a forma como o legislador, por um lado, ampliou de forma contundente o catálogo de crimes previsto no artigo 2º do Regime Jurídico das Ações Encobertas, e por outro, como passa a prever uma medida excecional para um enorme conjunto de crimes, sendo que alguns são de pequena criminalidade, sem aprofundar normativamente os princípios da necessidade e da proporcionalidade[93].

Para terminar devemos fazer uma breve referência a duas condutas a adotar neste tipo de medidas, que a ordem jurídico-criminal distingue, são elas a figura do *agente infiltrado* e do *agente provocador* (ambos agentes de polícia criminal). O primeiro pretende (Art. 5º do RJAE), com a sua atuação, ganhar a confiança do suspeito, tornando-se ele mesmo um criminoso, tendo assim acesso a planos, informações e dados que consubstanciem a prova de atos ilícitos. Quanto ao segundo, estamos a falar de uma entidade diferente, em que está em causa alguém que vai instigar à prática do crime[94]. No nosso ordenamento jurídico-penal este tipo de prova não é valorada, pois ocorre à margem da lei[95]. Importa só referir que, neste patamar, COSTA ANDRADE aponta uma terceira figura, o *Homem de Confiança*[96], em que se trata de alguém que colabora com a investigação, recolhendo informações do caso ou inserindo-se no meio.

---

[93] MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, p. 113.
[94] LAVOURA, Tiago Santos, *O agente infiltrado e o seu contributo para a investigação criminal*, Dissertação para obtenção do grau de Mestre em Ciências Jurídico-Forenses, orientado pelo Prof. Dr. Figueiredo Dias, e coorientado pela Mestre Ana Pais, Coimbra, Instituto Superior Bissaya Barreto, pp. 21 – 22.
[95] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II, *Bruscamente, A(s) Face(s) Ocultas dos Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010, p. 130.
[96] "*Na esteira de MEYER, adoptaremos aqui um conceito extensivo, abrangendo todas as testemunhas que colaboram com as instâncias formais da perseguição penal, tendo como contrapartida a promessa da confidencialidade da sua identidade e actividade. Cabem aqui tanto os particulares (pertencentes ou não ao submundo da criminalidade) como os agentes das instâncias formais, nomeadamente da policia (… agentes encobertos ou infiltrados), que disfarçadamente se introduzem naquele submundo ou com ele entram em contacto; e quer se limitem à recolha de informações (…), quer vão ao ponto de provocar eles próprios a prática do crime*" *In* ANDRADE, Manuel da Costa, *Sobre as Proibições de Prova em Processo Penal*, 2013, Coimbra Editora, p. 220.

6. O Arguido e a Prova Digital

6.1. Os Direitos do Arguido no Processo Penal

O processo penal português é um processo de sujeitos, os sujeitos processuais, e entre estes destaca-se arguido. Trata-se da pessoa visada no processo, aquele que se suspeita ter sido o agente do crime e contra quem é promovido o processo, com vista a apurar se o praticou, e nesse caso, ser-lhe aplicada a sanção criminal devida.

Para ser arguido não basta que sobre si recaia a suspeita de ter praticado o crime; é necessário que formalmente lhe seja atribuído esse estatuto no processo. Esse ato de atribuição da condição de arguido pode decorrer de um ato próprio ou adquirir-se automaticamente *ope legis*, quando for praticado um certo ato processual.

O arguido, pelo facto de o ser, é titular de direitos processuais[97]. Estes direitos encontram-se, plasmados no CPP em vários artigos, mas alguns encontram-se condensados no artigo 61º, n.º 1, do CPP, artigo este que cumpre diversos preceitos Constitucionais, como o artigo 32º da CRP ("Garantias de processo criminal").

Neste sentido, podemos começar por dizer que todos estes direitos do arguido, visam assegurar um verdadeiro (1) *direito de defesa* no processo penal. Este direito de defesa constitui uma verdadeira "*categoria aberta*"[98], que partindo da ideia de MARIA JOÃO ANTUNES[99], no cumprimento do *princípio do contraditório*, identificamos um (2) *direito ao contraditório* do arguido. Deste direito, emanam outros, que o CPP consagra, tais como: o direito de estar presente em todos atos processuais que diretamente lhe disserem respeito (Art. 61º, n.º 1, al. a), do CPP); o direito de ser ouvido pelo tribunal ou pelo juiz de instrução sempre que ele deva tomar qualquer decisão que pessoalmente o afete (Art. 61º, n.º 1, al. b), do CPP); o direito de intervir oferecendo provas e requerendo as diligencias que se lhe

---

[97] Segundo FIGUEIREDO DIAS e NUNO BRANDÃO, sendo o arguido um sujeito processual, tem um "*estatuto assente em três eixos fundamentais: o direito de defesa, garantido em geral, pelo art.32º/1 da CRP e depois concretizado por um sem numero de normas constitucionais e legais; o direito à presunção de inocência até ao transito em julgado da sentença de condenação, assegurado pelo art.32.º/2 da CRP; e o respeito pela decisão de vontade do arguido, manifestado essencialmente num direito à não autoincriminação." In* DIAS, Jorge de Figueiredo, BRANDÃO, Nuno, *Sujeitos Processuais Penais: o Arguido e o Defensor*, Texto de apoio ao estudo da unidade curricular de Direito Processual Penal do Mestrado em Ciências Jurídico-Forenses da Faculdade de Direito da Universidade de Coimbra, Coimbra, FDUC, 2020, p. 27.

[98] ANTUNES, Maria João, *Direito Processual Penal*, Almedina, 2017, pp. 39 – 41.

[99] Cfr. *Ibidem*, pp. 39 – 40.

afigurem necessárias (Art. 61º, n.º 1, al. g), do CPP); direito às ultimas declarações (Art. 361º, n.º 1, do CPP); direito de ser informado dos factos que lhe são imputados antes de prestar declarações perante qualquer entidade (Art. 61º, n.º 1, al. d), do CPP); direito de constituir advogado ou solicitar a nomeação de um defensor (Art. 61º, n.º 1, al. e), do CPP); de ser assistido por um defensor em todos os atos processuais que participar, e de poder comunicar com ele mesmo detido (Art. 61º, n.º 1, al. f), do CPP); de ser informado pela autoridade judiciária competente ou pelo OPC, dos direitos que lhe assistem, de não ser condenado por factos que alterem não substancialmente os descritos na acusação ou na pronúncia, sem se poder defender previamente (Art. 61º, n.º 1, al. h), do CPP); de não ser condenado por factos que alterem substancialmente os descritos na acusação ou na pronúncia; de recorrer das decisões que lhe forem desfavoráveis (Art. 61º, n.º 1, al. i), do CPP); o direito de requerer a abertura de instrução (Art. 287º, n.º 1, al. a), do CPP); o direito de requerer a intervenção do tribunal de júri (Art. 13º do CPP); e também o direito de se opor à desistência de queixa ou da acusação particular, podendo por esta via ver a sua inocência declarada em julgamento (Art. 51º do CPP).

Algo que está inerente à condição de arguido, no nosso processo penal, é a (3) *presunção de inocência*[100]. Na CRP, no artigo 32º, n.º 2, encontramos plasmado que "*Todo o arguido se presume inocente até ao transito em julgado da sentença de condenação (…)*". O arguido, à partida, deve ser tratado não como sendo culpado, mas sim como inocente. Este princípio é absolutamente estruturante e justifica o processo, pois é devido à presunção de inocência que há processo, e como tal, deve-se partir do princípio de que o arguido é inocente. Enquanto não houver prova de culpa, não há pena, e só após o trânsito em julgado, com o início da execução da pena, é que é levantada esta presunção.

No decorrer do processo, o arguido não pode ser sujeito a quaisquer sanções pelos factos que lhe são imputados, não havendo limitações ao seus direitos fundamentais, exceto, as medidas de coação previstas no CPP (Art. 196 e ss.). Embora aqui possa haver uma exceção, pois no caso de necessidade e adequação, estas limitações podem vir a ser efetivadas, por meio de lei. (como vamos ver e analisar mais à frente).

Do decorrer deste princípio, encontramos o (4) *direito ao silêncio* (Art. 61º, n.º 1, da al. d) do CPP). Um direito que abrange todas as fases do processo, no qual partimos da ideia de que o silêncio não pode ser alvo de qualquer tipo de valoração, não pode ser interpretado

[100] Já abordado também na p. 10.

como manifestação de culpa, estando em causa uma espécie de "nulo jurídico". Este direito encontra efetivação no âmbito das declarações do arguido, quer seja em sentido positivo quer negativo. O arguido tem o direito a prestar declarações[101], mas também, se assim o pretender, não está obrigado a falar, ou sequer a entregar documentos, acerca dos factos que lhe são imputados[102]. Podemos referir uma vertente mais ampla, ainda dentro do direito a não entregar documentos ou a ter de agir de determinada forma, onde VÂNIA COSTA RAMOS[103] afirma que "*sem o direito ao silêncio o arguido seria obrigado a declarar e a cooperar sempre que estes atos não revestissem conteúdo autoincriminatório*"

Deste último, e com uma clara ligação umbilical, partimos para outro direito, que assume enorme relevância nesta matéria, que é o chamado (5) *direito à não autoincriminação* (o princípio da proibição da não autoincriminação, *nemo tenetur se ipsum accusare*, Art. 58º, n.º 1, al. b), do CPP). Na linha que este direito encerra, o arguido no processo penal não pode ser coagido ou induzido em erro de forma a prestar declaração probatória no processo. Processo aqui diz respeito a todas as formas de prova que recaiam sobre o arguido, implicando um *facere*. Isto não quer dizer que não se possa autoincriminar, o que se impõe é que, se e quando o fizer, seja por meio de confissão, livre e informada (Art. 344º do CPP). É do entendimento geral, que este direito abrange também a figura do suspeito que ainda não tenha sido constituído arguido.

Em Portugal, no que diz respeito à afirmação deste princípio, encontramos uma corrente *processualista* como dominante, que defende que este princípio advém das garantias processuais do arguido (Art. 20º, n.º 4, Art. 32º, n.º 2, e n.º 8, da CRP), e do já referido, direito ao silêncio (Art. 58º, n.º 2, Art. 132º, n.º 2 e Art. 141º n. 4, do CPP). Esta também defende que este princípio protege os direitos fundamentais referidos pela corrente *substantivista* (onde o fundamento se encontra nos Art.s 1º, 25º, e 26º da CRP) [104].

O Tribunal Europeu dos Direitos do Homem afirma que este princípio deriva do chamado "*direito ao processo equitativo*", presente no artigo 6º, n.º 1, da CEDH (do mesmo modo que o direito ao silêncio). Neste sentido, e apesar de tal facto não estar expressamente

---

[101] COSTA ANDRADE neste sentido "*o arguido não pode ser fraudulentamente induzido ou coagido a contribuir para a sua condenação*" *In* ANDRADE, Manuel da Costa, *Sobre as proibições de prova em processo penal*, Coimbra Editora, 2013, p. 121.

[102] Cfr. com os artigos 61º, n.º 1, al. c), e 343º, n.º 1, ambos do CPP.

[103] RAMOS, Vânia Costa, «Imposição ao arguido de entrega de documentos para prova e nemo tenetur se ipsum accusare», Revista do Ministério Público, N.º 108, 2006, p. 132.

[104] DIAS, Figueiredo, ANDRADE, Manuel da Costa, *Supervisão, direito ao silêncio e legalidade de prova*, *Estudos Sobre o Mercado de Valores Mobiliários*, Coimbra Editora, 2009, pp. 41 – 42.

mencionado, o direito ao silêncio e o direito à não autoincriminação "*constituem standards internacionais que se situam no coração da noção de «processo equitativo» (fair procedure), tendo na sua razão de ser a ideia de proteção do acusado contra o exercício impróprio de poderes coercivos pelas autoridades, enquanto condição essencial ao acautelamento do perigo de adulteração da justiça e, neste sentido, à própria realização plena do espírito do art. 6.º da Convenção*"[105].

No que diz respeito à aplicabilidade, este Tribunal entende que este direito recai sob quem esteja numa "*posição substancialmente afetada por uma acusação de sentido equivalente ao da suspeita que oficialmente lhe é atribuída pelas autoridades*"[106].

Importa saber, que no ordenamento jurídico português, encontramos exceções previstas na lei, onde este princípio é restringido, em prol de outros interesses que devem ser salvaguardados[107] (e também através da aplicação do Art. 18º, n.º 2, da CRP, como iremos ver de seguida).

A posição do arguido ao longo dos últimos anos tem estado cada vez mais fragilizada. Os seus direitos são cada vez mais postos em causa com a chegada dos chamados "*meios ocultos de investigação*"[108]. Na opinião de RENATO LOPES MILITÃO, o crescimento destes leva a uma "*progressiva degradação das garantias processuais do suspeito e do arguido. De facto, a diminuição das garantias processuais é um dos aspetos que mais rapidamente se manifestam enquanto características do Estado punitivo. Efetivamente, sobreposto o valor segurança ao bem liberdade, os direitos fundamentais tendem a constituir um obstáculo numa luta eficaz do Estado contra a criminalidade. Assim o processo penal neoliberal é cada vez mais secretista, intrusivo e desleal*"[109].

---

[105] COSTA, Joana, «O princípio nemo tenetur na Jurisprudência do Tribunal Europeu dos Direitos do Homem.», Revista do Ministério Público n.º 128, 2011, pp. 117 – 118.
[106] *Ibidem*, p. 180.
[107] No que diz respeito a este tema o legislador, com intervenção do princípio da proporcionalidade (plasmado na CRP, no artigo 18º, n.º 2), já nos deu alguns exemplos: *Exames de alcoolemia e substâncias psicotrópicas* (Art. 152º, n.º 3, do Código da Estrada); *Exames de ADN para fins de investigação criminal* (172º do CPP e Art.º 8º da Lei n.º 4/2008) – Cfr. com Ac. Tribunal Constitucional, n.º 155/2007, Processo n.º 695/06.
[108] "*Efetivamente, foi nas últimas duas décadas que estes meios apareceram em massa e em força e se instalaram definitivamente no processo penal*" *In* MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 254.
Para COSTA ANRADE estes meios são "*todos aqueles métodos que representam uma intromissão nos processos de acçao, interação informação e comunicação das pessoas concretamente visadas*" *In* ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado", a reforma do Código de Processo Penal*, Coimbra Editora, 2009, p. 105.
[109] MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 255.

Nesta linha, e sendo considerados (os direitos fundamentais) um obstáculo que pode limitar a obtenção de prova digital, a forma encontrada para o superar, é restringi-los[110], para assim dar continuidade à investigação e ao processo penal, mesmo que assim se ponham em causa determinados direitos, e como já referimos, fragilizando a posição do arguido.

6.2. A Restrição de Direitos Fundamentais.

Segundo GOMES CANOTILHO "*a primeira função dos direitos fundamentais – sobretudo os direitos, liberdades e garantias – é a defesa da pessoa humana e da sua dignidade perante os poderes do Estado*"[111]. Na mesma linha, podemos colocar os direitos fundamentais num "*plano juridico-objectivo"* onde se tratam de *"normas de competência negativa para os poderes públicos proibindo fundamentalmente as ingerências destes na esfera jurídica individual"*, ou, noutro sentido, *"num plano juridico-subjectivo"*, onde implicam *"o poder de exercer positivamente direitos fundamentais (liberdade positiva) e de exigir omissões dos poderes públicos, de forma a evitar agressões lesivas por parte dos mesmos (liberdade negativa)*"[112].

O ordenamento jurídico português encerra o entendimento de que os direitos fundamentais só excecionalmente podem ser restringidos. Dispõe o artigo 18º, n.º 2, da CRP, 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*". Essas restrições devem partir de leis com "*carácter geral e abstrato e não podem ter efeito retroativo nem diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais*"[113].

---

[110] "*Além de precisarem de autorização constitucional, as restrições de direitos fundamentais carecem também de justificação, não podendo legitimar-se senão pela necessidade de salvaguardar outros direitos ou interesses constitucionalmente protegidos e não podendo ultrapassar a medida necessária para o efeito (art. 18.º-2). (…) Os direitos fundamentais só podem ser restringidos quando tal se torne indispensável, e no mínimo necessário, para salvaguardar outros direitos ou interesses constitucionalmente protegidos."*. "*A regra de solução do conflito é a da máxima observância dos direitos fundamentais envolvidos e da sua mínima restrição compatível com a salvaguarda adequada do outro direito fundamental ou outro interesse constitucional em causa*" *In* MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», pp. 269 – 270.
[111] CANOTILHO, Gomes, *Direito Constitucional e Teoria da Constituição*, Almedina, 2003, pp. 407 – 408.
[112] *Ibidem*, pp. 407 – 408.
[113] Art. 18º, n.º 3, da CRP.

No nosso entender, a prova digital assume uma posição agressiva quanto aos Direitos Fundamentais. Ao utilizarmos a prova digital como meio de prova ou como ferramenta, corremos o risco de ofender ou restringir este tipo de direitos[114]. Deste modo, há uma colisão de interesses: de um lado os direitos fundamentais dos cidadãos e do outro as finalidades do processo penal[115].

Mas tal como já vimos e frisámos, estes direitos não são absolutos[116] e era impensável imaginar a vida em sociedade se não fossem previstos mecanismos que pudessem limitar materialmente alguns direitos fundamentais, embora sempre, e muito importante, nunca colocando em causa o *princípio da dignidade da pessoa humana* (Art. 1º da CRP), constituindo este o limite máximo de qualquer restrição. Assim todos os cidadãos têm acesso aos mesmos direitos, servindo esta "*limitação interna*" como "*garante para uma igualdade a todos os cidadãos, de modo a que, todos tenham o mesmo acesso a ver protegidos os seus direitos*"[117].

É também importante frisar que, para haver restrição de direitos fundamentais, há mais uma exigência que deve ser cumprida: a competência especifica (Art. 165º, n.º 1, al. b), da CRP). É da exclusiva competência da Assembleia da República, salvo autorização ao Governo, legislar sobre matéria que recaia sobre Direitos Liberdades e Garantias.

6.3. A Restrição de Direitos nos Meios de Obtenção de Prova Digital

Atualmente, e como temos vindo a referir ao longo deste estudo, a importância assumida pelo uso de computadores (e sistemas equiparados), e a dimensão que esse uso atinge, seja a nível de comunicações, armazenamento e transferência de dados, é clara. Mas ao fazermos a associação destas duas matérias neste tópico (os direitos fundamentais e a

[114] Aqui podemos fazer referência a direitos constitucionalmente previstos, como por exemplo: o direito à imagem (Art. 26º, da CRP); o direito a inviolabilidade do domicílio informático (Art. 34º, da CRP), o direito á reserva da intimidade da vida privada e familiar, entre outros.
[115] Já referidas na p. 9.
[116] "*Efetivamente, os direitos fundamentais não são absolutos, podendo ser restringidos nos casos expressamente previstos na Constituição (art. 18º, n.º 2, 1ª parte). Esta autorização expressa legitima a atividade restritiva do legislador ordinário e dá segurança jurídica aos cidadãos, na medida em que apenas nesses casos poderá haver compreensão dos direitos fundamentais*", *In* CORREIA, João, «Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32, nº8, 2ª parte da CRP?)», Revista do Ministério Público, n.º 79, 1999, p. 59.
[117] ALMEIDA, Ivo Filipe de, *A Prova Digital*, Librum Editora, 2018, p. 71.

prova digital), o que pretendemos é saber se, com a investigação criminal em ambiente digital, onde se acede aos dados informáticos de um arguido, se este se encontra obrigado a colaborar com as autoridades, concedendo acesso aos seus dados (por exemplo à sua *password*[118], algo que é do conhecimento único de cada utilizador), ou, se neste caso estaremos perante uma restrição de algum principio constitucional, (como o caso do já visto princípio da não autoincriminação do arguido).

Para dar resposta a esta questão, retomamos a já estudada Lei do Cibercrime. Esta, como referimos, divide-se em três partes: a primeira que tem prevista um catálogo de crimes informáticos; a segunda de teor processual, prescreve os meios de obtenção de prova digital; e a terceira, que diz respeito à cooperação internacional. Para o nosso próximo ponto de estudo, são os meios de obtenção de prova que relevam, e quanto a estes (os elencados nos Art.s 12º ao 17º da LC), sabemos que o seu âmbito de aplicação recai sobre: o catálogo de crimes aí previstos, os que foram praticados por algum meio tecnológico, e aqueles em que seja necessário recolher prova em formato digital. Ficam apenas de fora a interceção de comunicações e as ações encobertas (Art.s 18º e 19 da LC).

Isto claramente demonstra que a maior parte dos meios de obtenção de prova que se encontram plasmados na Lei do Cibercrime podem ser aplicados à generalidade dos processos crime, desde que haja uma ligação ao meio informático e que seja claro o interesse na prova em formato digital. RENATO LOPES MILITÃO refere a este propósito, que embora a incidência destes meios de prova recaia "*sobretudo no domínio da cibercriminalidade, a questão da prova digital está longe de se esgotar aí. Coloca-se relativamente a todos os tipos criminais*"[119].

Seguindo a linha deste autor, e partindo das suas palavras, quando diz que "*pelas próprias características e potencialidades das NTIC, a concretização de tais medidas ofende, acrescida e gravemente múltiplos direitos, liberdades e garantias, não só dos agentes dos crimes, mas também, pelo menos em boa parte dos casos, de suspeitos inocentes ou terceiros acidentais*"[120], isto leva-nos a ponderar sob de que forma são feitas essas ofensas e que bens jurídicos são postos em causa.

---

[118] Palavra-passe: sequência de caracteres que identificam o utilizador de um computador e/ou permitem o acesso a dados, programas ou sistemas informáticos protegidos, *in* www.infopedia.pt.
[119] MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», p. 266.
[120] *Ibidem*, p. 267.

Vamos agora ver, e interligando com o que já foi dito anteriormente, de que forma os cidadãos, mas mais importante no nosso caso, o arguido, têm os seus direitos restringidos, quando está em causa um determinado meio de obtenção de prova digital.

a) Preservação e revelação expedita de dados de tráfego

A preservação expedita de dados, consiste na não eliminação e proteção da integridade de dados informáticos contra alterações ou destruição, não estando em causa o acesso aos mesmos. O simples salvaguardar dos dados não restringe qualquer direito fundamental[121]. Quanto ao elenco sobre qual pode ser ordenada, o legislador não o definiu, mas na linha RODRIGUES NUNES[122], devemos aplicar analogicamente a norma do artigo 187º, n.º 4, do CPP, alargando esta medida á figura do arguido, do suspeito, e à vítima.

No que diz respeito à revelação expedita, é obvia a sua dependência face à preservação expedita de dados, pois visa garantir a eficácia desta. E tal como na anterior, estando em causa dados de tráfego armazenados que já foram recolhidos, no que concerne à restrição de direitos fundamentais, lançamos mão dos mesmos argumentos e podemos dizer que, também aqui, não há restrição de qualquer direito fundamental. Quanto a saber sobre quem recai esta medida, e tendo em conta o carácter acessório que já referimos da norma, aplicam-se as mesmas regras do elenco que referimos para a preservação expedita de dados (Art. 187º, n.º 4, do CPP).

b) Injunção para apresentação ou concessão de acesso a dados

Neste caso, temos presente a medida que consagra que as autoridades judiciárias possam ordenar a quem tenha disponibilidade ou controlo de certos dados informáticos e que se encontrem armazenados num determinado sistema informático, que os comunique ao processo ou que permitam o acesso aos mesmos. Temos aqui uma resposta às dificuldades sentidas ao longo da investigação criminal quanto ao acesso a dados, que geralmente se encontram armazenados em sistemas informáticos com grande capacidade de armazenamento, o que leva a que seja mais difícil identificar os dados que concretamente se procuram, recaindo sob a pessoa visada pela injunção o dever de os transmitir ou conceder acesso.

[121] VERDELHO, Pedro, «A nova Lei do Cibercrime», Scientia Iuridica, Tomo LVIII, n.º 320, p. 736.
[122] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, Gestlegal, 2018, p. 46.

Apesar de esta medida ser menos invasiva do que uma pesquisa a um sistema informático (vamos analisar de seguida), a sua utilização implica que só as autoridades competentes tenham acesso a dados informáticos, o que nos demonstra que estão restringidos direitos fundamentais. Vemos uma restrição ao direito da intimidade e privacidade e ao direito à autodeterminação informacional. Importa ressalvar que neste caso o direito à inviolabilidade das comunicações não se considera restringido, pois o artigo 14º, n.º 4, da Lei do Cibercrime proíbe a obtenção de dados de conteúdo e tráfego[123].

No n.º 5, do artigo 14º da LC temos presente uma opção clara do legislador em salvaguardar o *direito à não autoincriminação,* quando deixa de fora do leque de pessoas alvo desta medida o arguido e o suspeito. Aqui o arguido não terá de ceder ou transmitir dados que o possam incriminar.

Impõe-se aqui outra questão, a de saber se a injunção poderá ser aplicada não a quem é diretamente arguido, mas antes a quem tenha o controlo informático do seus dados, seja por razão pessoal ou por mera organização empresarial, ou seja, se quem colaborar com o arguido poderá ser coagido a apresentar ou a facultar o acesso a dados do arguido. PEDRO VERDELHO[124] afirma que é possível exigir o acesso a computadores de empregados de empresas em que haja nos sistemas informáticos prova de atividades ilícitas. Assim podemos facilmente constatar que o legislador pretendeu apenas proteger o direito à não autoincriminação, pois continua a ser possível obter os dados do arguido, embora de outra forma.

c) <u>Pesquisa e Apreensão de dados informáticos</u>

A pesquisa de dados informáticos é um meio de obtenção de prova bastante invasivo, pois comporta o acesso a conteúdo de dados de qualquer natureza, acedendo de forma indiscriminada a todos os dados que se encontrem num determinado sistema informático. Deste modo, e devido ao modo como decorre, é obvio que estão restringidos direitos fundamentais, tais como inviolabilidade das comunicações (ainda que não intercetadas, podem estar no sistema informático) e o direito à privacidade informática.

No que diz respeito à apreensão de dados, também temos presente o acesso ao conteúdo de dados informáticos de qualquer natureza, mas com a diferença que neste caso

[123] *Ibidem*, p. 69.
[124] VERDELHO, Pedro, «A nova Lei do Cibercrime», Scientia Iuridica, Tomo LVIII, n.º 320, p. 739.

os dados apreendidos já serão só os necessários para a descoberta da verdade material[125]. Assim, e mesmo sendo de forma menos apertada, vemos restringidos os mesmos direitos que acima referimos para as pesquisas de dados.

Ao contrário do que pudemos ver para a injunção, aqui já não há nenhuma exceção ligada ao arguido. Partindo das palavras de RITA CASTANHEIRA NEVES e HÉLDER SANTOS CORREIA, está presente o entendimento que tem sido afirmado pelos tribunais e pela doutrina, de que existe "*uma natural delimitação negativa do direito à não autoincriminação, sempre que a prova em causa seja passível de ser obtida independentemente da vontade do arguido*" [126]. Assim, e estando disponíveis independentemente da colaboração do arguido, não é colocada na sua disponibilidade "*a possibilidade de se pesquisarem e apreenderem os objetos, documentos e comunicações, encontrem-se em suporte físico ou informático*"[127].

Importa, por último, saber se o arguido deve revelar ou não a sua palavra passe de qualquer sistema informático que lhe pertença, em matéria de pesquisas e apreensões de dados. Para responder a esta questão voltamos a citar os autores que referimos anteriormente pois, seguindo o seu entendimento, "*o que poderá estar em causa é o acesso por parte das autoridades judiciárias aos dados informáticos ser imediato ou diferido, já que a não colaboração do arguido apenas conduz à necessidade de apreender o suporte onde está instalado o sistema ou onde estão armazenados os dados do computador, que é uma das formas de executar a diligência prevista no artigo 16º da Lei do Cibercrime*"[128]. O legislador não previu qualquer dever de colaboração neste caso, não havendo nenhuma restrição do princípio da não autoincriminação[129].

Assim, mesmo que haja recusa do arguido, esta não limita o acesso das autoridades aos dados informáticos pois mesmo não tendo acesso à palavra chave, podem apreender o dispositivo e proceder ao *desbloqueio técnico*[130]. Podemos ainda acrescentar que, no que diz

[125] Isto no caso de não haver já acesso indiscriminado a todos os dados armazenados num sistema informático ou num suporte de armazenamento informático independentemente da causa, como acontece na pesquisa de dados, Cfr. NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, Gestlegal, 2018, p. 120.
[126] NEVES, Rita Castanheira, CORREIA, Hélder Santos, «A lei do cibercrime e a colaboração do arguido no acesso aos dados informáticos», Actualidad Juridica Uría Menendez, 2014, p. 149.
[127] *Ibidem*, p. 149.
[128] *Ibidem*, p. 149.
[129] Acerca deste tópico da "*Revelação Coativa da password*" ver CORREIA, João Conde, «Prova digital: as leis que temos e a lei que devíamos ter», Revista do Ministério Público, n.º 139, 2014, pp. 58 – 59.
[130] NEVES, Rita Castanheira, CORREIA, Hélder Santos, «A lei do cibercrime e a colaboração do arguido no acesso aos dados informáticos», Actualidad Juridica Uría Menendez, 2014, p. 149.

respeito ao arguido, se no decurso de uma diligência, recusar facultar o acesso ao correio eletrónico, não estando ele num computador, mas sim na web (na internet), "*mesmo que o arguido se recuse a colaborar com a investigação, não revelando de sua vontade a palavra-passe destas contas de email, o legislador legitimou as autoridades judiciárias a intervir diretamente junto do servidor dessa conta*"[131].

d) Apreensão de correio eletrónico

Ao contrário dos outros meios de prova que analisamos até agora, e mesmo sendo uma norma especial face ao artigo 16º da LC, este meio de obtenção de prova recai sobre o correio eletrónico ou registos de comunicações de natureza semelhante, que se encontrem armazenados num sistema informático, a que a autoridade irá ter acesso. Importa referir que o consentimento para que as autoridades tenham acesso à prova, transcrevam e juntem aos autos, faz com que não seja necessária a aplicação do preceituado no artigo 17º da LC.

Como já referimos anteriormente, este meio de prova é dos que suscita mais divergências doutrinais. Um dos motivos dessa discussão será no seu âmbito de aplicação. No que diz respeito a esta matéria, aplicam-se o artigo 17º da LC, e subsidiariamente, conforme o plasmado no mesmo, o regime do artigo. 179º do CPP.

Este meio de obtenção de prova comporta o acesso ao conteúdo de dados informáticos no formato de mensagens de correio eletrónico ou equiparado (como já referimos: *SMS*[132], *Messenger*, *WhatsApp*, *Facebook*, entre outros). É importante ressalvar que o acesso de que estamos a falar recai sobre os dados que sejam estritamente necessários para a investigação e procura da verdade material, não estando nunca em causa um acesso indiscriminado e sem limites à totalidade de dados presentes no sistema informático ou suporte de armazenamento em questão (como podemos ver no caso da pesquisa de dados informáticos). Assim, neste caso, os direitos que estão postos em causa são fundamentalmente o direito à intimidade e privacidade, e segundo RODRIGUES NUNES[133], o direito à palavra virtual e à autodeterminação informacional.

---

[131] *Ibidem*, p. 149.
[132] Cfr. MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, p. 119, Nota n.º 74.
[133] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, Gestlegal, 2018, p. 147.

Por último, importa dizer que a apreensão apenas poderá ser feita se tiver alguma ligação ao arguido ou ao suspeito, seja como destinatário ou expedidor. A este propósito remetemos para o artigo 17º da LC e para o regime do artigo 179º, n.º 1, al. a), do CPP[134].

e) Interceção de comunicações e as ações encobertas

Optei por analisar este dois meios de prova em conjunto apenas pela sua exclusão no âmbito de aplicação do artigo 11º da LC.

No preceito do artigo 18º da Lei n.º 109/2009, está prevista a interceção de comunicações informáticas. É feita sobre um sistema informático, e importa a captação de informações, sejam dados de conteúdo de comunicações ou os dados de tráfego (em tempo real ou de dados conservados nos termos da Lei n.º 32/2008). Esta interceção, nas palavras de RODRIGUES NUNES "*configura uma restrição de direitos fundamentais, que será especialmente intensa no caso do acesso aos dados de conteúdo e de grau não tão intenso nos dados de tráfego*"[135]. Nesta linha, importa realçar o facto de que esta medida apenas deve ser aplicada "*se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outro modo, impossível ou muito difícil de obter*"[136], pois quando é exercida é especialmente danosa, ou seja, há um acesso indiscriminado a todos os dados de conteúdo e de tráfego de comunicações que sejam efetuados pelo o visado, quando for utilizado o sistema informático que esteja a ser alvo deste meio de prova. O visado, neste caso, e segundo o artigo 187º, n. 4, do CPP, pode ser o arguido, o suspeito, o intermediário e a vítima (mediante consentimento).

Podemos assim dizer que com a aplicação deste meio de obtenção de prova são restringidos os direitos: à privacidade informática, à inviolabilidade das comunicações, à autodeterminação informacional, à liberdade de expressão e à palavra virtual[137] e o direito à confidencialidade e integridade dos sistemas técnico-informacionais[138].

---

[134] "*apenas poderão ser apreendidas mensagens de correio eletrónico ou de outras realidades análogas que tenham sido enviadas pelo arguido ou suspeito ou que lhe tenham sido dirigidas*" *in* NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, Gestlegal, 2018, p. 151.

[135] NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, Gestlegal, 2018, p. 160.

[136] Art. 18º, n.º 4 da LC, que remete para o 187º do CPP.

[137] Cfr. VENÂNCIO, Pedro Dias, *Lei do Cibercrime: Anotada e Comentada*, 2011, Coimbra Editora, p. 199, e NEVES, Rita Castanheira, *As Ingerências nas Comunicações Eletrónicas em Processo Penal natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prov*a, Coimbra Editora, 2011 p. 277.

[138] Cfr. ANDRADE, Manuel da Costa, *"Bruscamente no Verão Passado", a reforma do Código de Processo Penal*, Coimbra Editora, 2009, p. 165, e NEVES, Rita Castanheira, *As Ingerências nas Comunicações*

No artigo seguinte (Art. 19º da LC), com a epigrafe "Ações Encobertas", está presente a regulação das ações encobertas em ambiente digital[139]. Trata-se de uma criação do legislador português, pois tal como a apreensão de correio eletrónico, não são medidas que se encontravam presentes na Convenção de Budapeste[140].

A ação encoberta é definida pelo artigo 1º, n.º 2, da Lei n.º 101/2001, de 25 de Agosto, como "*aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária*[141] *para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade*". No nosso caso, a ação encoberta insere-se no plano informático-digital.

Nesta matéria, assumem relevância as figuras do agente infiltrado, o agente provocador (e também o *homem de confiança*).

O meio de obtenção de prova digital nas ações encobertas, restringe os direitos fundamentais que referimos para a interceção de comunicações, se bem que podemos aqui acrescentar, como estando restringido também o direito à inviolabilidade do domicílio[142].

No que diz respeito aos sujeitos sob os quais poderá recair esta medida, a lógica será a mesma que para os meios de prova que já analisámos, ou seja, aplicamos o artigo 187º, n.º 4, do CPP. Assim identificamos o arguido, o suspeito, o intermediário, e a vítima (quando esta prestar consentimento).

Importa por último perguntarmo-nos: será que, ao admitirmos como prova as informações recolhidas numa ação encoberta com teor digital, estamos a violar o princípio da proibição da autoincriminação do arguido?

Para responder a esta questão, seguimos a linha de RODRIGUES NUNES[143]. Partimos do princípio de que o arguido deve ser informado antes de prestar declarações dos

---

*Eletrónicas em Processo Penal natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prov*a, Coimbra Editora, 2011, p. 241.

[139] Apesar de, na epigrafe do artigo 19º da LC constar apenas o termo Ações Encobertas "*a Doutrina vem-se a referindo a estas ações encobertas como «ações encobertas em ambiente informático-digital», a fim de as destrinçar das ações encobertas previstas na Lei n.º 101/2009*" *In* NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, Gestlegal, 2018, p. 196, Nota n.º 392.

[140] Já abordado na Nota n.º 52, p. 24.

[141] Segundo PAULO PINTO DE ALBUQUERQUE, podemos aqui incluir o Serviço de Estrangeiros e Fronteiras também como competente, nos casos em que a competência para investigação recaia sobre o SEF, Cfr. ALBUQUERQUE, Paulo Pinto de, *Comentário ao Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 2011, p. 681.

[142] "*embora apenas quando implique a entrada num espaço que goze da tutela deste direito*" *In* NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, Gestlegal, 2018, p. 205.

[143] *Ibidem*, pp. 210 – 215.

factos que lhe são imputados, e como já vimos, este tem sempre direito a não prestar quaisquer declarações, tem o direito ao silêncio. O arguido, pelo facto de o ser, tem um amplo leque de direitos que o protegem e o acompanham ao longo dos interrogatórios do processo penal. Mas aplicamos estes preceitos ao "interrogatório" da ações encobertas? Na opinião do autor (que nós seguimos), não se aplicam, pelo menos diretamente "*aos «interrogatórios» realizados pelo agente infiltrado, que, pelo seu caráter informal (usualmente realizado no decurso de uma conversação normal entre duas pessoas que confiam uma na outra), poderão levar o interlocutor a fornecer informações autoincriminatórias ou cujo fornecimento poderia validamente recusar num interrogatório formal. Daí que se trate de uma questão extremamente controversa*"[144].

O arguido não conhece a qualidade do agente infiltrado, e este, cumprindo o seu papel, deve manter essa qualidade oculta, não estando obrigado a transmitir ou informá-lo das condições e direitos da qualidade de arguido. Neste sentido "*jamais se poderá falar de fornecimento de elementos falsos acerca de depoimentos ou outros elementos fácticos existentes nos autos para determinar o interrogado a modificar as suas declarações*"[145]. E, importa também dizer, que no caso de o agente infiltrado advertir o arguido da sua qualidade, ele estaria aqui a pôr em causa a característica mais importante da investigação, o desconhecimento da identidade do agente infiltrado.

O autor realça que não estamos perante uma violação do princípio *nemo tenetur*, por duas razões: em primeiro lugar quando se recorre, numa investigação, a agentes infiltrados, a sua atuação geralmente ocorre antes de que as testemunhas ou o arguido possam sequer recusar-se a depor; e por outro lado, este princípio não abrange "*descuidos*"[146], e seria demais estar a ampliar o princípio a este tipo de situações.

Posto isto, podemos afirmar que as declarações do agente infiltrado que tiverem origem no âmbito das ações encobertas, poderão ser usadas como prova no processo penal.

[144] *Ibidem*, p. 211.
[145] *Ibidem*, p. 213.
[146] Neste sentido "descuido" é o arguido confiar no agente e nesse sentido confidenciar-lhe a prática de um crime.

II – CONCLUSÃO

A tecnologia é o motor da sociedade contemporânea; o nosso quotidiano está afincadamente marcado por ela, seja no que diz respeito à ciência, ao trabalho ou ao lazer. As evoluções e a presença tecnológica são inegáveis em todos os domínios, e como pudemos analisar ao longo deste estudo, também chegou ao direito penal.

A Internet tem sido um grande marco na evolução da humanidade, mas trata-se de um "pau de dois bicos", pois nem tudo o que nos trouxe foi certamente positivo. Com isto a criminalidade também evoluiu ganhando uma nova faceta e armas (digitais). Assistimos ao surgimento de um novo catálogo de crimes em ambiente informático-digital, e ao aparecimento de novas formas de realizar alguns tipos de crime de outra natureza, já anteriormente tipificados.

De forma a responder a este tipo de criminalidade foi necessária a implementação de medidas que permitissem fazer-lhe frente, combatê-la. A recolha de Prova Digital tornou-se imperativa. Em Portugal, a primeira arma que surgiu foi a Lei n.º 109/91, a Lei da Criminalidade Informática.

Com o passar dos anos esta tornou-se inapropriada para lidar com os avanços tecnológicos que se fizeram sentir.

Também a nível internacional surgiu uma resposta, na Convenção do Cibercrime, em Budapeste a 23 de Novembro de 2003, que só foi transposta para o nosso país em 2009, pela atual Lei do Cibercrime, a Lei n.º 109/2009, de 15 de Setembro.

Esta nova Lei veio revogar a anterior, 18 anos depois. Trouxe alterações significativas a nível material, com o catálogo de crimes (trouxe alguns da lei da cibercriminalidade), também a nível processual, com a criação de meios de obtenção de prova digital, e com medidas de cooperação internacional.

É importante também fazer referência à Lei n.º 32/2008, que trata da Conservação de dados gerados ou tratados no contexto de oferta de serviços de comunicações eletrónicas.

Contudo, é de notar que não concordamos com esta dispersão legislativa, onde as disposições processuais constam de legislação especial, quando se deveriam encontrar no diploma central de processo penal português, o CPP. Apontamos aqui DÁ MESQUITA[147]

[147] Já referido na Nota n.º 54, p. 25.

quando refere que seria benéfico esta matéria estar regulada no CPP, no Livro III, relativo à prova (Título III), criando-se um capítulo dedicado à Prova Digital (um novo Capítulo V), pois esta também se aplica a outros crimes, além dos consagrados na Lei do Cibercrime; o autor fala também, no caso de opinião contrária, ao invés do já dito, que se considerasse uma remissão no CPP para esta Lei.

No que diz respeito às novidades a nível processual que a Lei do Cibercrime nos trouxe, temos consagrados nos artigos 12º a 19º dessa mesma lei, como pudemos ver e analisar ao longo deste estudo, os meios de obtenção de prova digital.

O legislador português seguiu a linha do conteúdo da Convenção do Cibercrime para a implementação destas medidas. Encontramos neste leque a pesquisa e revelação expedita de dados de tráfego, a injunção para apresentação ou concessão do acesso a dados, a pesquisa e apreensão de dados informáticos, e também a interceção de comunicações. Mas em dois casos de originalidade, o legislador português acrescentou a este leque os meios da Apreensão de Correio Eletrónico (Art. 17º da LC), e as Ações Encobertas (Art. 19º da LC).

Por outro lado, o legislador não previu como meio de obtenção de prova as *buscas online*. Na esteira de RITA CASTANHEIRA NEVES[148], definem-se como um método oculto de investigação, segundo o qual os dados informáticos do dispositivo tecnológico do visado seriam recolhidos ocultamente, sem que ele tivesse conhecimento. Tendemos a concordar com alguns autores que defendem a sua presença na LC como um meio válido, e extremamente útil à investigação criminal, apesar do carácter extremamente invasivo que apresenta. É claro que, para poder vigorar na nossa ordem jurídica, teria de estar envolto em inúmeros prossupostos, com tutela jurisdicional.

Com a chegada da Lei do Cibercrime garantiu-se um reforço na proteção de bens jurídicos, como por exemplo a privacidade informática, a integridade informática, até o domicílio informático (que já se encontravam protegidos pela Lei nº 109/91, a Lei da Criminalidade Informática). Daqui surgiram novos desafios no que diz respeito ao processo penal e à prova. Mas tal como a prova tradicional, a prova de cariz digital deve seguir os princípios gerais de direito, e tanto a sua valoração como a restrição devem sempre ter em

[148] NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas em processo penal: natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*, Coimbra Editora, 2011, pp. 198, 284, 351.

conta os direitos fundamentais consagrados na CRP. Essa restrição deve ser realizada conforme o artigo 18º, n.º 2, da CRP.

Como pudemos analisar ao longo deste estudo, partimos do princípio que estes direitos, ao não serem absolutos, podem ser restringidos com a aplicação dos meios de obtenção de prova digital, quando estejam em causa interesses como o bom curso da investigação e a descoberta da verdade material.

Uma dúvida quanto ao tema das restrições, a qual pudemos analisar, prendia-se com a figura do arguido, mais concretamente em saber se os seus direitos também podem ser restringidos no âmbito da investigação digital, e de que forma se mantém o direito da não autoincriminação deste, bem assente durante toda a investigação.

No que concerne aos meios de obtenção de prova digital, podemos referir que a posição do arguido se encontra, logicamente, atacada. Há bens jurídicos que, tal como referimos nesta dissertação, são postos em causa com a aplicação destas medidas. Apesar disso, defendemos que o seu núcleo central de direitos e garantias se mantém, no sentido em que há direitos que são preservados, como por exemplo o direito da não autoincriminação.

Deste modo, e dando por terminada esta investigação, é importante frisar que com a veloz e gigantesca evolução tecnológica a que temos assistido nos últimos anos, podemos assumidamente esperar que as NTIC vão impor sempre novos e complicados desafios ao Direito Penal. Resta esperar que em face da crítica à lei processual penal que tem vindo a ser produzida, e toda a análise que tem sido feita ao regime de prova digital, o nosso direito evolua por forma a superar todas as vicissitudes que este longo caminho trouxer, sempre com a ideia de não se deixar ficar para trás e dar resposta pronta e eficaz a todos esses avanços tecnológicos.

III – BIBLIOGRAFIA

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

- ALMEIDA, Ivo Filipe de, *A Prova Digital*, Librum Editora, 2018.

- ANDRADE, Manuel da Costa, *Bruscamente no Verão Passado, a reforma do Código de Processo Penal*, Coimbra Editora, 2009.

- ANDRADE, Manuel da Costa, *Sobre as proibições de prova em processo penal*, Coimbra Editora, 2013.

- CANCELA, Alberto Gil Lima, *A Prova Digital: os Meios de Obtenção de Prova na Lei do Cibercrime*, Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra, sob orientação da Prof. Dra. Sónia Fidalgo, Coimbra, 2016.

- CANOTILHO, Gomes, *Direito Constitucional e Teoria da Constituição*, Almedina, 2003.

- CARDOSO, Rui, «Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15/IX», Revista do Ministério Público, n.º 153, 2018, pp. 167 – 214.

- CORREIA, João Conde, «Prova digital: as leis que temos e a lei que devíamos ter», Revista do Ministério Público, n.º 139, 2014, pp. 29 – 59.

- CORREIA, João Conde, «Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32, nº8, 2ª parte da CRP?)», Revista do Ministério Público, n.º 79, 1999, pp. 45 – 67.

- COSTA, Joana, «O princípio nemo tenetur na Jurisprudência do Tribunal Europeu dos Direitos do Homem.», Revista do Ministério Público n.º 128, 2011, pp. 117 – 183.

- COSTA, José Francisco de Faria, *Algumas reflexões sobre o estudo dogmático do chamado "Direito Penal Informático", Direito Penal da Comunicação, alguns escritos*, Coimbra Editora, 1998.

- DECO, *Internet e vida Privada, Proteja os seus dados pessoais*, Edições DECO Proteste, 2016.

- DIAS, Figueiredo, *Direito Processual Penal*, Coimbra Editora, 2004.

- DIAS, Figueiredo, *Direito Processual Penal*, Lições coligidas por Maria João Antunes, Secção de textos da Faculdade de Direito da Universidade de Coimbra, 1988-89.

- DIAS, Figueiredo, ANDRADE, Manuel da Costa, Supervisão, *Direito ao silêncio e legalidade de prova, Estudos Sobre o Mercado de Valores Mobiliários,* Coimbra Editora, 2009.

- DIAS, Jorge de Figueiredo, BRANDÃO, Nuno, *Sujeitos Processuais Penais: o Arguido e o Defensor, Texto de apoio ao estudo da unidade curricular de Direito Processual Penal do Mestrado em Ciências Jurídico-Forenses da Faculdade de Direito da Universidade de Coimbra*, Coimbra, FDUC, 2020, disponível em https://apps.uc.pt/mypage/files/nbrandao/2226 .

- FERREIRA, Manuel Cavaleiro de, *Curso de Processual Penal, II vol*., Editora Danúbio, 1986.

- FIDALGO, Sónia, «A apreensão de correio electrónico e a utilização noutro processo das mensagens apreendidas», Revista Portuguesa de Ciência Criminal, n.º 29, 2019, pp. 59 – 74.

- FREITAS, José Pedro, *Os Meios de Obtenção de Prova Digital na Investigação Criminal: O regime jurídico dos serviços de correio eletrónico e de mensagens curtas*, NOVA CAUSA Edições Jurídicas, 2020.

- JESUS, Francisco Marcolino de, *Os Meios de Obtenção de Prova*, Almedina, 2ª Edição, 2019.

- LAVOURA, Tiago Santos, *O agente infiltrado e o seu contributo para a investigação criminal*, Dissertação para obtenção do grau de Mestre em Ciências Jurídico-Forenses, orientado pelo Prof. Dr. Figueiredo Dias, e coorientado pela Mestre Ana Pais, Coimbra, Instituto Superior Bissaya Barreto, 2012.

- MACEDO, João Carlos Cruz Barbosa de, *Direito Penal hoje: novos desafios e novas respostas*, Coimbra Editora, 2009.

- MARQUES, Garcia, MARTINS, Lourenço, *Direito da Informática*, Almedina, 2006.

- MENDES, Paulo de Sousa, "*As proibições de prova no processo penal"*, *Jornadas de Direito Processual e Direitos Fundamentais*, Almedina, 2004.

- MESQUITA, Paulo Dá, *Processo Penal, Prova e Sistema Judiciário*, Wolters Kluwer / Coimbra Editora, 2010, pp. 83 – 129.

- MILITÃO, Renato Lopes, «A propósito da prova digital no processo penal», Revista da Ordem dos Advogados, ano 72, n.º 1, 2012, p. 247 – 285, disponível em: https://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf.

- NEVES, Rita Castanheira, *As ingerências nas comunicações electrónicas em processo penal: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prov*a, Coimbra Editora, 2011.

- NEVES, Rita Castanheira, CORREIA, Hélder Santos, «A lei do cibercrime e a colaboração do arguido no acesso aos dados informáticos», Actualidad Juridica Uría Menendez, 2014, pp. 146 – 149.

- NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na lei do cibercrime*, Gestlegal, 2018, pp. 213.

- PEREIRA, Alexandre Dias, *Direito da Informática, Estudo, Vol. I,* FDUC, disponível em https://eg.uc.pt/bitstream/10316/87707/1/Direito%20da%20Inform%C3%A1tica%20Estudos%20Vol%20I.pdf .

- RAMALHO, David, *Métodos ocultos de investigação criminal em ambiente digital*, Almedina, 2017.

- RAMALHO, David, «A investigação criminal da Dark Web», *in* Revista da Concorrência e Regulação, Ano 4, n.º 14/15, 2013.

- RAMOS, Armando Dias, *A Prova Digital em Processo Penal, O Correio Eletrónico*, Chiado Editora, 2014.

- RAMOS, Vânia Costa, «Imposição ao arguido de entrega de documentos para prova e nemo tenetur se ipsum accusare», Revista do Ministério Público, N.º 108, 2006, pp. 125 – 149.

- RIBEIRO, Maria da Conceição Fernandes, *Cibercrime e Prova Digital*, Dissertação apresentada ao Instituto Superior Bissaya Barreto, Coimbra, 2015.

- RODRIGUES, Benjamim Silva, *Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital*, Coimbra Editora, 2009.

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

- RODRIGUES, Benjamim Silva, *Da Prova Penal – Tomo IV, Da Prova Eletrónico-Digital e da Criminalidade informático-Digital*, Rei dos Livros, 2011.

- SANTOS, Cristina Máximo dos, «As Novas Tecnologias da Informação e o Sigilo das Telecomunicações», separata da Revista do Ministério Público, n.º 99, Lisboa, 2004, p. 96.

- SANTOS, Rita Coelho dos, *O Tratamento Jurídico-Penal da Transferência de Fundos Monetários através da Manipulação Ilícita dos Sistemas Informáticos*, Coimbra Editora, 2005.

- VENÂNCIO, Pedro Dias, *Lei do Cibercrime: Anotada e Comentada*, Coimbra Editora, 2010.

- VENÂNCIO, Pedro Dias, «As medidas da prova digital da Lei do Cibercrime – regra ou exceção», Boletim da Ordem dos Advogados, n.º 123, Fevereiro de 2015, pp. 40 – 41.

- VERDELHO, Pedro, «A nova Lei do Cibercrime», Scientia Iuridica, Tomo LVIII, n.º 320, 2009, pp. 717 – 749.

- VERDELHO, Pedro, "Cibercrime", *Direito de Sociedade da informação, Vol. IV, APDI*, Coimbra Editora, 2003.

- VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes; *Leis do Cibercrime, Vol. 1*, p. 18, excerto disponível em http://www.centroatl.pt/titulos/direito/imagens/excerto-ca-leisdocibercrime1.pdf .

Outros Documentos Relevantes

- Fórum "Direitos Fundamentais nos Processos Penais na Europa", de 16.09.2006, disponível em : http://www.oa.pt/upl/%7Bb37359b4-47e1-425a-957b-3d27584ba679%7D.pdf .

- Nota Pratica nº8/2016, de 18 de Fevereiro de 2016, "Pedido de dados a operadores de comunicações", do gabinete de Cibercrime do Ministério Público, disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_pedido_de_info_a_isp_0.pdf .

- Nota Prática nº16/2020, de 19 de Março de 2020, Jurisprudência sobre Prova Digital, do gabinete de Cibercrime do Ministério Público, disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_16_jurisprudencia_prova_digital.pdf .

- Parecer do Conselho Consultivo da PGR, com o n.º Convencional PGRP00003238, Relator: PAULO DÁ MESQUITA, 2012, disponível em: http://www.dgsi.pt/pgrp.nsf/f1cdb56ced3fdd9f802568c0004061b6/a734913d16b0f89480257af00043b68a?OpenDocument .

- Relatório Anual de Segurança Interna, Ano de 2019, disponível em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3D%3DBQAAAB%2BLCAAAAAAABAAzNDA0sAAAQJ%2BleAUAAAA%3D .

- Relatório Anual de Segurança Interna, Ano de 2017, disponível em: http://www.ansr.pt/InstrumentosDeGestao/Documents/11Relat%C3%B3rio%20Anual%20de%20Seguran%C3%A7a%20Interna%20(RASI)/RASI%202017.pdf .

IV – JURISPRUDÊNCIA

- Ac. do Tribunal da Relação de Évora, de 20-01-2015, Processo n.º 648/14.6GCFAR-A.E1, com relator JOÃO GOMES DE SOUSA, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument .

- Ac. do Tribunal da Relação de Guimarães, de 29-03-2011, Processo n.º 735/10.0GAPTL-A.G1, com relator MARIA JOSÉ NOGUEIRA, disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument .

- Ac. do Tribunal da Relação de Lisboa, de 07-03-2018, Processo n.º 184/12.5TELSB-B.L1-3, com relator CONCEIÇÃO GONÇALVES, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument .
- Ac. do Tribunal da Relação de Lisboa, de 06-02-2018, Processo n.º 1950/17.0T9LSB-A.L1-5, com relator JOÃO CARROLA, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument .
- Ac. do STJ de 3/03/2010, Processo n.º 886/07.8PSLSB.L1.S1, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25061d49157a048c8025770a002ed7d7?OpenDocument .
- Ac. Tribunal Constitucional, n.º 155/2007, Processo n.º 695/06, disponível em: https://dre.pt/home/-/dre/2068880/details/maximized .