Prova digital: Articulação entre o Código de Processo Penal Português e a Lei do Cibercrime

Digital Proof: Articulation between the Portuguese Code of Criminal Procedure and Cybercrime Law

Joaquim Ramalho
Doutor em Direito pela Faculdad de Ciencias Jurídicas y del Trabajo, Universidad de Vigo, Espanha. Mestre em Direito pela Faculdade de Direito da Universidade do Porto, Portugal. Licenciado em Direito pela Faculdade de Direito da Universidade do Porto, Portugal. Professor Associado na Faculdade de Ciências Humanas e Sociais, Universidade Fernando Pessoa, Portugal. Investigador no Observatório Permanente de Violência e Crime, Universidade Fernando Pessoa, Portugal. Advogado.

Resumo: O cibercrime é, nos tempos hodiernos, uma das principais ameaças à segurança nacional e internacional. É um crime que ultrapassa fronteiras e, deste modo, têm vindo a surgir diplomas legislativos internacionais de combate a este tipo de crime, os quais podem colidir com as legislações nacionais. Um dos principais pontos de colisão reside na articulação entre o regime especial da Lei do Cibercrime e o regime geral Código de Processo Penal, nomeadamente no que respeita à pesquisa de dados informáticos e às perícias e exames informáticos. A opção pelo regime especial poderia fazer supor que este sobrepõe ao regime geral, no entanto, demonstra-se que o regime especial não invalida o regime geral, já que estamos perante um regime processual de obtenção de prova digital com um campo de aplicação mais abrangente do que a própria lei.

Palavras-chave: Cibercrime; Pesquisa de dados informáticos; Perícias informáticas; Exames informáticos

Abstract: Cybercrime is, in modern epochs, one of the main fears to national and global security. It is a crime that crosses borders, and, in this way, international legislation has been emerging to combat this type of crime, which end up colliding with national law. One of the main points of collision lies in the articulation between the special regime of the Cybercrime Law and the general regime of the Criminal Procedure Code, namely about computer data research and computer expertise and exams. The option for special regime could lead to the assumption that it overlaps the general regime, however, it is shown that the special regime does not invalidate the general regime, since we are dealing with a procedural regime for obtaining digital evidence with a larger field of application than the law itself.

Keywords: Cybercrime; Computer data search; Computer expertise; Computer exams

1. Introdução

É inegável a relevância que as novas tecnologias apresentam na vida dos cidadãos. Normalmente,

são utilizadas em benefício dos seus utilizadores, permitindo que, em segundos, se possa ter acesso a informação contida em qualquer parte do mundo. No entanto, as novas tecnologias não acarretam apenas vantagens. A utilização universal de correio eletrónico ou de redes sociais, entre outras, constituem um meio de acesso à prática de crimes tradicionais[1], mas com recurso às tecnologias, mas constituem também numa retumbante proliferação de determinados tipos de criminalidade.

Com a revolução tecnológica foram alterados os tipos de contacto entre as pessoas, surgindo novas redes relacionais e, por consequência, também novas formas de crime, como, por exemplo, a criminalidade informática[2], designada de cibercrime.

Foi na época pós-moderna, com a revolução tecnológica e com a globalização, que o ciberespaço - o qual diz respeito a um espaço existente no universo de comunicação, através do qual não é necessária a presença física para constituir uma comunicação relacional - ganhou preponderância, ao funcionar como um espaço de partilha de informações e de contacto entre pessoas de todo o mundo.

A criação da internet, no ano de 1969, veio ajudar a consolidar um mundo sem fronteiras espaciais, territoriais, sociais, económicas e linguísticas, surgindo a designada sociedade de informação. Com o aparecimento da cibernética, da digitalização e, sobretudo, de uma comunidade com uma cibercultura e com ciberespaço, surge a chamada sociedade digital[3].

De acordo com a Procuradoria-Geral da República[4], as denúncias de cibercrime, em sentido amplo, têm vindo a aumentar, de uma forma consistente, desde o ano de 2016. No ano de 2020, ano de pandemia da COVID-19, as denúncias aumentaram de uma forma excecional, no entanto, o aumento foi ainda mais expressivo no ano de 2021, revelando que entre janeiro e dezembro foram recebidas 1160 denúncias, enquanto no ano anterior foram registadas 544 denúncias, ou seja, de ano para ano, as denúncias têm vindo a duplicar.

Ainda de acordo com a mesma fonte, a criminalidade mais frequente é a seguinte: *phishing*, burlas online, burlas com páginas "falsas", burlas com criptoativos e outros produtos financeiros, burlas em relações pessoais, CEO *fraud*, ataques informáticos, falsas chamadas da Microsoft®, divulgação de fotografias e outra informação pessoal, stalking e sextortion, discurso de ódio online, violação de direitos de autor, crimes contra a honra e defraudações na utilização da aplicação de pagamentos MBWAY®.

Para promover o combate à cibercriminalidade, a europa tem vindo a aprimorar a legislação e, em 2009, com a publicação da Lei nº 109/2009 de 15 de setembro, Portugal transpôs para a ordem interna a Decisão-Quadro nº 2005/222/JAI do Conselho da Europa.

2 Cibercrime

O crime caracteriza-se como sendo um facto humano, normalmente voluntário, declarado punível pela norma jurídica. Formalmente, o crime é uma ação ou um facto típico, ilícito e culposo. Materialmente, crime é todo o comportamento humano que lesa ou ameaça de lesão (coloca em perigo)

[1] Como, por exemplo, crimes como a burla, a injúria ou as ameaças.
[2] As constantes disseminações de vírus informáticos são um exemplo.
[3] MARQUES DIAS, V. A problemática da investigação do cibercrime. **Data Venia, Revista Jurídica Digital**, 1 (1), 2012, p. 63-88.
[4] PROCURADORIA-GERAL DA REPÚBLICA. **Cibercrime: denúncias recebidas**. Lisboa: Ministério Público de Portugal. 2022.

bens jurídicos fundamentais.

Atualmente, uma das principais formas de crime é, sem dúvida o cibercrime que é hoje uma das principais ameaças ao respeito pelos Direitos Fundamentais dos cidadãos, podendo até ser, por variadas razões uma ameaça à segurança interna e internacional[5].

Procurando definir cibercriminalidade, podemos referir que, de acordo com a Comissão Europeia[6], entende-se por cibercrime os atos criminosos praticados com recurso a redes comunicacionais eletrónicas e sistemas de informação ou contra este tipo de redes ou sistemas.

Acrescente-se que o cibercrime corresponde, em termos gerais, à designação dada aos crimes cibernéticos que envolvam qualquer tipo de atividade ou de prática ilícita na rede, sendo que essas práticas podem envolver, por exemplo, a disseminação de vírus, a falsidade informática, as invasões de sistema, o roubo de dados pessoais ou o acesso a informações confidenciais[7].

Coelho dos Santos[8], apresenta uma classificação tripartida, nos termos da qual distingue: (a) os crimes tipicamente informáticos, que correspondem aqueles que o legislador reconhece, em sentido amplíssimo, como sendo crimes eminentemente ligados à informática, na medida em que o objeto ou instrumento da ação é um computador ou outro equipamento tecnologicamente semelhante; (b) os crimes essencialmente informáticos, que compreendem unicamente aqueles em que o próprio bem jurídico ofendido consiste numa realidade de natureza informática e que possui dignidade suficiente para merecer a tutela penal; (c) os crimes acidentalmente informáticos, que são aqueles crimes em que a utilização do computador é apenas um *modus operandi*, não contendendo, em si, o preenchimento do respetivo tipo legal.

Mais recentemente, para Marques Dias[9] e Rodrigues Nunes[10], a sistematização da cibercriminalidade pode ser entendida seguindo 2 prismas diferentes: (a) por um lado, pode ser perspetivada num sentido amplo, englobando todos os ilícitos criminais praticados através de meios informáticos, em que a eles sejam reconduzidos todo e qualquer facto tipificado na lei como crime e que seja praticado através da utilização de um sistema informático, com base no artº 2.º a) da Lei do Cibercrime, a Lei nº 109/2009 de 15 de setembro; (b) por outro lado, num sentido mais restrito, englobando apenas os crimes cujo tipo legal pressupõe a prática de uma conduta criminosa através do uso de meios informáticos ou contra um bem informático, que a ele se subsuma apenas os crimes em que o sistema informático integra o tipo legal de crime ou surge como objeto de proteção, tal como, por exemplo, os crimes previstos na Lei nº 109/2009 de 15 de setembro ou a burla informática.

3 Fontes normativas internacionais do cibercrime

Como se pode perceber, tendo em conta a natureza e o âmbito global da cibercriminalidade, não

[5] RODRIGUES NUNES, D. **Os crimes previstos na lei do cibercrime**. Lisboa: Editora Gestlegal. 2020.
[6] COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões. Rumo a uma política geral de luta contra o cibercrime. In https://eur-lex.europa.eu. 2007.
[7] RODRIGUES NUNES, D. **Os crimes previstos na lei do cibercrime**. Lisboa: Editora Gestlegal. 2020.
[8] COELHO DOS SANTOS, R. O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos. **Boletim da Faculdade de Direito**. Coimbra: Coimbra Editora. 2005.
[9] MARQUES DIAS, V. A problemática da investigação do cibercrime. **Data Venia, Revista Jurídica Digital**, 1 (1), 2012. p. 63-88.
[10] RODRIGUES NUNES, D. **Os crimes previstos na lei do cibercrime**. Lisboa: Editora Gestlegal. 2020.

é difícil de encarar este tipo de crime como sendo um crime que, facilmente, ultrapassa fronteiras. Assim sendo, para além de legislação nacional que possa combater o cibercrime, é necessária a existência de instrumentos legais de cooperação internacional, porque só deste modo se poderá combater a cibercriminalidade de uma forma verdadeiramente eficaz.

No mundo e particularmente na europa, têm vindo a ser desenvolvidas diversas fontes normativas no que respeita à cibercriminalidade, dado que com o acelerar do avanço tecnológico, é necessário dar respostas eficientes e imediatas no combate a este tipo de crimes.

Através da Lei nº 109/2009 de 15 de setembro, designada de Lei do Cibercrime (doravante designada de LC), Portugal transpôs para a ordem interna a Decisão-Quadro nº 2005/222/JAI do Conselho da Europa, relativa a ataques contra sistemas de informação. No entanto, como veremos mais à frente, este regime especial tem vindo a causar alguns problemas de articulação com o regime geral do Código de Processo Penal em Portugal (doravante designado de CPP).

São quatro os principais diplomas internacionais que estiveram na base da atual LC, a Convenção sobre o Cibercrime do Conselho da Europa, Decisão-Quadro do Conselho Europeu e a Diretiva do Parlamento Europeu e do Conselho Europeu e a Lei nº 32/2008, de 17 de julho, os quais serão analisadas em seguida.

A Convenção sobre o Cibercrime do Conselho da Europa, de 23 de novembro de 2001, aberta à assinatura em Budapeste, teve como objetivo fundamental criar mecanismos destinados a proteger a sociedade contra a cibercriminalidade, designadamente através da adoção de legislação adequada que fomentasse também a cooperação internacional.

Procurou, com a previsão de normas penais substantivas e adjetivas, harmonizar as várias legislações dos países signatários, promovendo, assim, um combate mais eficaz contra a cibercriminalidade, ao contemplar um conjunto de conceitos informático-jurídicos, de ilícitos criminais, de medidas processuais destinadas a regular a forma de obtenção de prova em ambiente digital e de mecanismos de cooperação internacional.

Portugal subscreveu a Convenção sobre o Cibercrime em 2001, no entanto, só procedeu à sua ratificação em 2009, por Resolução da Assembleia da República nº 88/2009 e pelo Decreto do Presidente da República nº 92/2009, ambos publicados a 15 de setembro, data que corresponde à publicação da Lei nº 109/2009, de 15 de setembro.

A LC, como consta no próprio texto, adaptou ao direito interno a Convenção sobre o Cibercrime. Por este facto e pelo papel que teve e que continua a ter no combate contra a cibercriminalidade, era essencial mencioná-la na presente exposição.

Para além da Convenção sobre o Cibercrime atrás referida, que, sem qualquer dúvida, serviu de paradigma para a elaboração da LC, importa também destacar um outro diploma legal, a Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de fevereiro.

A Decisão-Quadro nº 2005/222/JAI do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, decorre das linhas orientadoras promovidas pela Convenção sobre o Cibercrime.

A Decisão-Quadro, tal como a Convenção, teve como fundamento o de procurar reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes, através da aproximação das disposições de direito penal no que respeita aos ataques contra os sistemas de informação, tendo em

atenção que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, o que faz realçar uma absoluta necessidade de harmonizar as legislações penais no âmbito da cibercriminalidade.

Este diploma legal estabelece, nos artº 2.º, 3.º e 4º, a incriminação de diversas condutas, como sejam, o acesso ilegal a sistemas de informação e de dados.

O legislador português transpôs esta Decisão-Quadro do Conselho da Europa e a Convenção sobre o Cibercrime do Conselho da Europa, através da Lei nº 109/2009 de 15 de setembro.

A Diretiva nº 2006/24/CE, do Parlamento e do Conselho, de 15 de julho[11], reporta-se à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou em redes públicas de comunicações.

Esta Diretiva foi transposta para a ordem jurídica portuguesa através da Lei nº 32/2008, de 17 de julho, que procura regular a conservação e a transmissão dos dados de tráfego e de localização, tal como os dados conexos necessários para identificar o assinante ou o utilizador registado para fins de investigação destes e repressão de crimes graves.

Como fomos percebendo, a globalização é vista como um agente facilitador dos crimes praticados por meios eletrónicos e, deste modo, no mundo e particularmente na europa, têm vindo a ser desenvolvidas diversas fontes normativas no que respeita à cibercriminalidade, uma vez que, tal como acrescenta Marques Dias[12], a diversidade de ordens jurídicas e a respetiva diferente qualificação do ilícito, levam a que à mesma conduta lesiva sejam aplicadas diferentes sanções ou até que a conduta seja vista como um ilícito criminal num país e não o seja noutro.

Contudo, até ao ano de 2009, Portugal não havia dado cumprimento aos diferentes preceitos de cariz internacional a que se encontrava vinculado, resultantes do facto de ter assinado, em 23 de novembro de 2001, a Convenção sobre o Cibercrime do Conselho da Europa, que, como vimos, é ainda hoje considerada como o primeiro e mais importante trabalho internacional versando a temática cibercrime.

Em 2009, com a publicação da Lei nº 109/2009 de 15 de setembro, Portugal transpôs para a ordem interna a Decisão-Quadro nº 2005/222/JAI do Conselho da Europa, relativa a ataques contra sistemas de informação[13], respeitando as obrigações internacionais a que o Estado Português estava adstrito, o legislador nacional consagrou, finalmente, um autêntico sistema processual de prova digital.

A LC foi inovadora, na medida em que instituiu, pela primeira vez, regras jurídicas específicas referentes à recolha de prova em suporte eletrónico. Até então, a investigação dos crimes relacionados com a informática fazia-se com recurso às normas pertinentes, interpretadas com as necessárias adaptações, do CPP. Com a aprovação desta lei, o legislador procurou reunir num único diploma todas as normas respeitantes à criminalidade informática, tais como, normas de direito substantivo, normas de direito processual e também normas relativas à cooperação judiciária em matéria penal[14].

Do ponto de vista estrutural, a LC possui um conjunto de normas de natureza adjetiva, designadas

[11] Esta Diretiva foi subsequentemente revogada e substituída pela Diretiva 2013/40/EU do Parlamento Europeu e do Conselho da Europa, de 12 de agosto, também relativa a ataques contra sistema de informação.
[12] MARQUES DIAS, V. A problemática da investigação do cibercrime. **Data Venia, Revista Jurídica Digital**, 1 (1), 2012. p. 63-88.
[13] Tal como refere o artº 1.º da Lei nº 109/2009 de 15 de setembro.
[14] Acórdão do Tribunal Constitucional. Processo número 830/2021.

como disposições processuais, estabelecendo uma série de novos meios de obtenção de prova. Contudo, embora tenha passado a consagrar um sistema processual de prova digital, a LC veio criar problemas de articulação com o CPP, uma vez que o legislador, ao duplicar os regimes, consagrou o regime geral do CPP e o regime especial da LC.

Um dos exemplos de duplicação - e de possível contradição - na articulação entre os dois regimes, designadamente, tal como refere Conde Correia[15], na aplicação do regime especial da LC e o regime geral do CPP, entre a pesquisa de dados informáticos (artº 15.º da LC) e as perícias (artº 151.º e segs do CPP) e os exames (artº 171.º e segs do CPP).

Deste modo, a grande questão da presente investigação consiste em perceber se, doutrinalmente, a LC revogou, de uma forma tácita, o CPP, persistindo apenas este regime geral no que não estiver especialmente consagrado, dado que, tal como sustenta o autor supra citado, uma vez que a norma do artº 11.º da LC determina, pela via positiva, o âmbito de aplicação processual das disposições nela constantes, e exclui, pela via negativa, a aplicação de qualquer outra lei para estes crimes, incluindo, naturalmente, o CPP, ou seja, a única forma de aceder ao conteúdo de um computador seria através da pesquisa de dados informáticos (artº 15.º LC), pelo que, todas as outras formas de acesso seriam ilegitimamente ordenadas, inviabilizando assim a realização de meios de prova (perícias informáticas) e meios de obtenção de prova (exames).

Tendo em conta o problema doutrinal em estudo, será analisado, de seguida, o regime de acesso à prova digital no processo penal português e as respetivas dificuldades de articulação entre os regimes supra citados.

4 Prova digital: dificuldades na articulação entre o Código de Processo Penal Português e a Lei do Cibercrime

Como ponto prévio, é importante reconhecer que a reflexão acerca da construção da prova enquanto forma de reconstrução da verdade foi sempre um tema imensamente debatido no domínio do Direito Processual Penal. Um dos seus princípios basilares consiste no princípio da legalidade ou legitimidade da prova, conforme estabelece o artº 125.º do CPP.

Tal como refere o artº supra citado, todas as provas são admissíveis, excetuando as que são proibidas pela lei (o que densifica o estabelecido constitucionalmente, designadamente o que postula o artº 32.º/8 e 34.º/4 da Constituição da República Portuguesa, doravante designada de CRP). Ambos os artigos proíbem, de uma forma expressa, a admissão de provas obtidas, *verbi gratia*, mediante tortura, coação, ofensa à integridade física ou moral ou abusivas intromissões na vida privada, no domicílio, na correspondência e nas telecomunicações.

Destes princípios resulta o exposto no artº 126.º/1 e 3 do CPP, que só vem compactar o que determina a CRP, mencionando que são nulas, as provas obtidas mediante tortura, coação ou com ofensa da integridade física das pessoas e ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas as provas obtidas mediante intromissão na vida privada, no domicílio, na

[15] CONDE CORREIA, J. Prova digital: enquadramento legal. In: **Cibercriminalidade e prova digital. Jurisdição penal e processual penal**. Lisboa: Centro de Estudos Judiciários, 2020. pp. 23-37.

correspondência e nas telecomunicações sem o consentimento do respetivo titular[16].

É de notar que o regime legal da prova está codificado no CPP, o qual inclui os meios de prova e os meios de obtenção de prova. Embora uma parte deste livro seja dedicado a este tema, o código não apresenta qualquer conceito de prova, limitando a sua referência ao objeto da prova.

No âmbito do Direito Civil, o Código Civil português, no artº 341.º, expressa uma definição mais especifica de prova, referindo que, as provas têm por função a demonstração da realidade dos factos, demonstrando os elementos da realidade pelos meios intelectivos permitidos por lei, tendo como principal finalidade formar a convicção do juiz sobre os elementos necessários para a decisão da causa.

Realçando a importância da prova em toda a investigação, determina-se que depois de adquirida a notícia do crime e aberto o inquérito, ocorrem um conjunto de diligências que constituem os fundamentos principais da prova, ou seja, a indagação da existência ou inexistência de um crime, a determinação de responsabilidade do seu agente e a recolha de provas, de modo obter uma decisão sobre a possível acusação[17].

De acordo com Simas Santos & Leal-Henriques[18], a prova consiste na atividade que se destina a demonstrar a verdade dos factos ocorridos, ou seja, é um processo direto que permite obter a justificação da convicção sobre a existência de um determinado facto.

Como referido, no âmbito do Direito Processual Penal português, podemos distinguir os meios de prova dos meios de obtenção de prova. Os meios de obtenção de prova são os instrumentos de que se servem as autoridades judiciárias para investigar e recolher meios de prova. Os meios de prova correspondem aos caminhos através dos quais se desenvolve a atividade probatória, destinada à demonstração dos factos relevantes relacionados com o crime que se pretende investigar. Por outro lado, os meios de obtenção de prova correspondem às diversas diligências realizadas pelas autoridades, de modo a recolher prova.

De modo a estabelecer uma diferenciação mais proficiente, Marques da Silva[19], estabelece a distinção entre os meios de prova e os meios da sua obtenção, mencionando o seguinte que parece claro que através meios de obtenção de prova se podem obter meios de prova de diferentes espécies, por exemplo, documentos, coisas, indicação de testemunhas, mas o que releva de modo particular é que, nalguns casos, o próprio meio de obtenção da prova acaba por ser também um meio de prova.

O CPP, no artº 124.º, faz uma distinção entre os meios de prova e os meios de obtenção de prova, mencionando que se constituem objeto de prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança a aplicar.

Num sentido restrito e direto, a prova é a demonstração explicita da realidade de um facto ou da existência de um ato jurídico, será também o processo ou o conjunto dos procedimentos que tem por fim tal demonstração. Ou seja, podemos ver a prova como resultado ou a prova como demonstração.

Conforme atrás referido, os meios de prova e de obtenção de prova previstos no CPP que, de uma

[16] Acórdão do Tribunal da Relação de Lisboa. Processo número 351/20.8PZLSB-C.L1-5, de 09 de novembro de 2021.
[17] MARCOLINO DE JESUS, F. **Os meios de obtenção de prova em processo penal**. Coimbra: Almedina. 2015.
[18] SIMAS SANTOS, M.; LEAL-HENRIQUES, M. **Noções de Direito Processual Penal**. Porto: Editora Rei dos Livros. 2011.
[19] MARQUES DA SILVA, G. **Curso de Processo Penal – noções gerais, elementos do processo penal**. Volume I. Lisboa: Verbo Editora. 2010.

forma evidente, colidem com o regime especial de pesquisa de dados informáticos - artº 15.º da LC - são, respetivamente, as perícias e os exames informáticos.

Passando a analisar o artº 15.º da LC, relativo à pesquisa de dados informáticos. Refere o nº 1 desta norma que se durante uma investigação se revelar essencial para a descoberta da verdade obter determinados dados informáticos armazenados num sistema informático, a autoridade judiciária competente autoriza ou ordena, mediante despacho[20], a pesquisa de tais dados no sistema informático.

De acordo com um acórdão do Tribunal da Relação de Lisboa[21], a apreensão de dados informáticos a que a LC se refere não equivale à apreensão prevista no CPP, pela própria natureza das coisas. Esta última passa por desapossar alguém da coisa corpórea, enquanto a apreensão do conteúdo digital, bastas vezes virtual e armazenado num servidor em qualquer lugar do mundo, facilmente possibilita, especialmente quanto ao correio eletrónico, a continuação do acesso pelo utilizador original ao seu conteúdo, o qual, em bruto, é apenas linguagem binária.

Acrescenta esse mesmo acórdão que a apreensão de dados informáticos tem muito mais a ver com a respetiva perceção e assim apenas ocorre quando o conteúdo de mensagens de correio eletrónico é desvendado e junto ao processo em linguagem comum, uma vez que é apenas nesse momento que ocorre a efetiva compressão do direito à inviolabilidade da correspondência que a lei visa salvaguardar com as garantias e formalidades processuais que impõe, designadamente a da reserva judicial no que respeita àquela correspondência eletrónica.

Analisando, mais detalhadamente, cada um dos regimes, podemos mencionar que, tal como refere Marques da Silva[22], a perícia corresponde à atividade de perceção ou de apreciação dos factos probandos, efetuada por pessoas dotadas de especiais conhecimentos.

De acordo com a norma prevista no artº 151.º do CPP, a prova pericial ocorre quando a perceção ou a apreciação dos factos exigirem especiais conhecimentos técnicos, científicos ou artísticos, que determinará, posteriormente, a sua valoração (artº 163.º do CPP).

A perícia é realizada em estabelecimento, laboratório ou serviço oficial apropriado ou, quando tal não for possível ou conveniente, por perito nomeado de entre pessoas constantes de listas de peritos existentes em cada comarca, ou, na sua falta ou impossibilidade de resposta em tempo útil, por pessoa de honorabilidade e de reconhecida competência na matéria em causa (artº 152.º do CPP).

Quando a perícia se revelar de especial complexidade ou exigir conhecimentos de matérias distintas, pode ela ser deferida a vários peritos funcionando em moldes colegiais ou interdisciplinares.

Terminada a perícia, os peritos procedem à elaboração de um relatório, no qual mencionam e descrevem as suas respostas e conclusões devidamente fundamentadas. Aos peritos podem ser pedidos esclarecimentos pela autoridade judiciária, pelo arguido, pelo assistente, pelas partes civis e pelos consultores técnicos (artº 157.º do CPP).

Quanto ao valor da prova pericial (artº 163.º do CPP), o juízo técnico, científico ou artístico inerente à prova pericial presume-se subtraído à livre apreciação do julgador. Sempre que a convicção do julgador divergir do juízo contido no parecer dos peritos, deve aquele fundamentar a divergência.

---

[20] Acrescenta o nº 2 do artº 15.º da LC que este despacho tem a validade máxima de 30 dias, sob pena de nulidade.
[21] Acórdão do Tribunal da Relação de Lisboa. Processo número 351/20.8PZLSB-C.L1-5, de 09 de novembro de 2021.
[22] MARQUES DA SILVA, G. **Curso de Processo Penal – noções gerais, elementos do processo penal.** Volume I. Lisboa: Verbo Editora. 2010.

Analisando os exames, importa mencionar que é através de exames a pessoas, a lugares e a coisas que se inspecionam os vestígios que possa ter deixado a prática do crime, como sejam, ao modo como e ao lugar onde foi praticado, às pessoas que o cometera ou sobre as quais foi cometido (artº 171.º/1 do CPP).

Os exames podem ocorrer por iniciativa própria dos órgãos de polícia criminal (artº 55.º/2, 171.º/4 e 173.º do CPP), sem prejuízo de, aos exames suscetíveis de ofender o pudor das pessoas, só poder assistir a autoridade judiciária competente (artº 172.º/3, 270.º/2 e) e 290.º/2 do CPP).

Podem também ocorrer por competência de uma autoridade judiciária (juiz, juiz de instrução e Ministério Público, artº 1.º b) do CPP) em que esta obriga alguém que pretenda abstrair-se de realizar qualquer exame ou de facultar coisa que deva ser examinada (artº 172.º/1 do CPP).

É de competência reservada de um juiz, o exame que envolva as características físicas e/ou psíquicas de uma pessoa que não tenha prestado qualquer tipo de consentimento para a realização desses mesmos exames (artº 172.º/2 e artº 269.º/1 b) do CPP).

As perícias e os exames, quando são realizados a sistemas informáticos, apresentam limitações diversas, as quais resultam das especificidades que os acessos à prova digital encerram.

Devido à sua natureza, a prova digital apresenta caraterísticas que a diferenciam dos meios de obtenção de prova clássicos: (a) é uma prova de acesso complexo já que tem caráter temporário; (b) é fungível, uma vez que há uma enorme facilidade de substituição dos dados informáticos por outros; (c) é de natureza imaterial e volátil, dado que facilmente se escondem esses dados, podendo ser ocultados ou suprimidos, do suporte original e também é frágil, exigindo especiais cuidados no seu manuseamento, o que obriga, ao avaliador, conhecimentos técnicos e científicos elevados[23].

A prova digital pode ser definida como sendo a informação passível de ser extraída de um dispositivo eletrónico ou de uma rede de comunicações. Deste modo, a prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta[24].

A LC sistematizou processualmente, embora de uma forma não muito clara, o regime de prova digital. Tal como refere Conde Correia[25], passaram a reger-se pela LC a pesquisa de dados informáticos, a apreensão de dados informáticos, a apreensão de correio eletrónico e de registos de comunicações de natureza semelhante e a interceção de comunicações.

Conforme foi referido anteriormente, e conforme refere o autor supra mencionado, dado que o artº 11.º da LC determina, pela via positiva, o âmbito de aplicação processual das disposições nela constantes, e exclui, pela via negativa, a aplicação de qualquer outra lei para estes crimes, interessa perceber qual o regime que prevalece.

Apesar de a LC estabelecer, expressamente, no artº 11.º, a aplicação processual do regime especial, excluindo a aplicação de qualquer outro preceito legal, tal não se verifica na realidade, dado que o regime especial não invalida o regime geral, pois existem pressupostos e objetivos referentes à pesquisa informática, como a obtenção de dados informáticos específicos armazenados no computador,

[23] LOPES MILITÃO, R. A propósito da prova digital no processo penal. **Revista da Ordem dos Advogados**, 72 (5), 2012. p. 247-285.
[24] DIAS RAMOS, A. **A prova digital em Processo Penal.** Lisboa: Chiado Editora. 2014.
[25] CONDE CORREIA, J. Prova digital: enquadramento legal. In: **Cibercriminalidade e prova digital. Jurisdição penal e processual penal**, Lisboa: Centro de Estudos Judiciários, 2020. pp. 23-37.

que poderão carecer de perícias ou exames simultaneamente.

Nas palavras de Venâncio[26], as normas previstas nos artº 11.º e segs da LC possuem uma extensão geral, uma vez que estamos perante a possibilidade de recorrer a estes meios de obtenção de prova para combate à criminalidade em geral, independentemente da forma. Deste modo, tal como afirma o autor, estamos perante um regime processual de obtenção de prova digital com um campo de aplicação mais abrangente do que a própria lei porque não restringe a sua aplicação aos processos relativos aos crimes que nela estão contemplados.

Por tudo o que foi supracitado, somos levados a concordar com o que Verdelho[27] estabelecia, quando refere ser incorreto ver na figura da pesquisa de dados informáticos, algum tipo de substituto para os exames, uma vez que a própria LC reconhece a possibilidade de aplicação de outras leis, ao regular, nos artº 16.º e 17.º, a pesquisa informática ou de outro acesso legítimo a um sistema informático. Como tal, não será a única lei reguladora em matéria de aquisição processual de dados, afastando a exclusividade.

Como evidência do supra mencionado, em que se verifica a articulação da aplicação de diferentes regimes, num acórdão do Tribunal da Relação do Porto[28] estabelece-se que a busca de onde resulte a apreensão de um computador é regulada pelas normas do CPP. Por outro lado, a pesquisa dos dados informáticos num computador, bem como a apreensão desses mesmos dados, é regulada na LC.

Pelo supra citado, importa realçar que a lei também se aplica nas seguintes situações: (1) aos crimes praticados através de um sistema informático; (2) aos processos relativos a crimes em que seja necessário proceder à recolha de prova digital, no decorrer da investigação criminal.

Como reflexão, convém ainda realçar as palavras de Lopes Militão[29], revelando que se tem vindo a constatar uma progressiva degradação das garantias processuais do suspeito e do arguido, dado que, sobrepondo o valor da segurança à liberdade, os direitos fundamentais tendem a constituir um obstáculo numa luta eficaz dos Estados contra a criminalidade.

Acrescenta o autor que a LC, com o objetivo de obter prova digital, consagrou diversos meios processuais e mecanismos de cooperação internacional, os quais podem se tornar profundamente intrusivos e até mesmo indesejáveis. Deste modo, muito embora a LC tenha uma enorme importância no combate à cibercriminalidade, ao mesmo tempo pode originar a violação de Direitos Fundamentais, constitucionalmente previstos.

5 Considerações finais

Com efeito, reserva-se este capítulo final para uma síntese conclusiva de todo o trabalho assim como para uma reflexão sobre o mesmo.

Como mencionado, os meios de prova e de obtenção de prova constituem os alicerces que sustentam a construção da prova no processo penal. Enquanto uns são instrumentos de que se servem as

[26] VENÂNCIO, P. D. **Lei do Cibercrime: anotada e comentada**. Coimbra: Coimbra Editora. 2011.
[27] VERDELHO, P. **A nova lei do Cibercrime**. Tomo LVIII. Braga: Scientia Juridica. 2009.
[28] Acórdão do Tribunal da Relação do Porto. Processo número 2039/14.0JAPRT.P1, de 07 de julho de 2016.
[29] LOPES MILITÃO, R. A propósito da prova digital no processo penal. **Revista da Ordem dos Advogados**, 72 (5), 2012. p. 247-285.

autoridades judiciárias para investigar e recolher meios de prova, outros, permitem que a verdade dos factos possa ser obtida e avaliada, de forma constituir uma fonte de justificação devidamente fundamentada, com vista à aplicação de medidas aos agentes do crime.

Na prova digital, a LC veio superar uma lacuna que existia no ordenamento jurídico-penal em Portugal, no entanto, como não originou uma revogação expressa do CPP, criou problemas na articulação entre os dois diplomas, dado que, cumprindo um dos princípios basilares do Direito, dever-se-ia aplicar o regime na aplicação da LC, em detrimento do regime geral do CPP.

Em nosso entender - e concordando com a doutrina maioritária - o legislador, ao consagrar a o regime da prova digital na LC, pretende fornecer aos órgãos de polícia criminal instrumentos de combate à criminalidade em geral, pelo que nos parece ser incorreto, por exemplo, na norma da LC referente à pesquisa de dados informáticos, alguma forma de substituição para o consagrado no CPP para esta matéria, uma vez que a própria LC reconhece a possibilidade de aplicação de outras leis, distanciando-se, assim, da exclusividade de aplicação.

Referências bibliográficas

Literatura:

ALBUQUERQUE, P. P. **Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem**. 3ª edição atualizada. Lisboa: Universidade Católica Editora. 2015.

ANTUNES, M. J. **Consequências Jurídicas do Crime**. 1ª edição. Coimbra: Coimbra Editora. 2013.

COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões. **Rumo a uma política geral de luta contra o cibercrime**. Disponível em: https://eur-lex.europa.eu (consultado em 28 de dezembro de 2021). 2007.

COELHO DOS SANTOS, R. O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos. **Boletim da Faculdade de Direito**. Coimbra: Coimbra Editora. 2005.

CONDE CORREIA, J. Prova digital: enquadramento legal. In: **Cibercriminalidade e prova digital. Jurisdição penal e processual penal**, pp. 23-37. Lisboa: Centro de Estudos Judiciários. 2020.

DIAS RAMOS, A. **A prova digital em Processo Penal**. Lisboa: Chiado Editora. 2014.

FIGUEIREDO DIAS, J. **Direito Penal Português: Parte Geral II – As Consequências Jurídicas do Crime.** 2ª reimpressão. Coimbra: Coimbra Editora. 2011.

FIGUEIREDO DIAS, J. O Direito Penal do bem jurídico como princípio juridicoconstitucional implícito. **Revista de Legislação e Jurisprudência,** 3998, 144, 2016, p. 250-266.

LOPES MILITÃO, R. A propósito da prova digital no processo penal. **Revista da Ordem dos Advogados**, 72 (5), 2012. p. 247-285.

MARCOLINO DE JESUS, F. **Os meios de obtenção de prova em processo penal.** Coimbra: Almedina. 2015.

MARQUES DA SILVA, G. **Curso de Processo Penal – noções gerais, elementos do processo penal**. Volume I. Lisboa: Verbo Editora. 2010.

MARQUES DIAS, V. A problemática da investigação do cibercrime**. Data Venia, Revista Jurídica Digital,** 1 (1), 2014. p. 63-88.

MIRANDA RODRIGUES, A. **A determinação da medida da pena privativa da liberdade: os critérios da culpa e da prevenção**. 1ª edição. Coimbra: Coimbra Editora. 2014.

PROCURADORIA-GERAL DA REPÚBLICA. **Cibercrime: denúncias recebidas**. Lisboa: Ministério Público de Portugal. 2022.

RODRIGUES NUNES, D. **Os crimes previstos na lei do cibercrime**. Lisboa: Editora Gestlegal. 2020.

RODRIGUES NUNES, D. **Os meios de obtenção de prova previstos na lei do cibercrime**. Lisboa: Editora Gestlegal. 2018.

SILVA RAMALHO, D. A recolha de prova digital através de pesquisas informáticas transfronteiriças. In: **O domínio do imaterial: prova digital, cibercrime e a tutela penal dos direitos intelectuais. Jurisdição penal**, pp. 57-70. Lisboa: Centro de Estudos Judiciários. 2018.

SIMAS SANTOS, M. & Leal-Henriques, M. **Noções de Direito Penal.** 6ª edição. Porto: Editora Rei dos Livros. 2018.

SIMAS SANTOS, M. & Leal-Henriques, M. **Noções de Direito Processual Penal**. Porto: Editora Rei dos Livros. 2011.

VENÂNCIO, P. D. **Lei do Cibercrime: anotada e comentada**. Coimbra: Coimbra Editora. 2011.

VERDELHO, P. **A nova lei do Cibercrime**. Tomo LVIII. Braga: Scientia Juridica. 2009.

Jurisprudência:

Acórdão do Tribunal da Relação de Lisboa. Processo número 351/20.8PZLSB-C.L1-5, de 09 de novembro de 2021.

Acórdão do Tribunal Constitucional. Processo número 830/2021.

Acórdão do Tribunal da Relação do Porto. Processo número 2039/14.0JAPRT.P1, de 07 de julho de 2016.

Recebido em: 04/06/2022
Aprovado em: 29/07/2022