Recolha de prova em suporte eletrónico: os regimes do código de processo penal e a lei do cibercrime

Electronic evidence: Portuguese code of criminal procedure and cybercrime law regimes

10.29073/j2.v7i1.787

Recebido: 24 de julho de 2023.
Aprovado: 20 de março de 2024.
Publicação: X de X de 2024.

Autor: Joaquim Ramalho, Universidade Fernando Pessoa, Portugal, ramalho@ufp.edu.pt.

Resumo

O cibercrime é um crime que ultrapassa fronteiras e a sua prevalência tem vindo a aumentar nos últimos anos. Em Portugal, com a publicação da Lei do Cibercrime, passou a ter, para além do Código de Processo Penal, outro diploma legal destinado a prevenir e combater a criminalidade informática, no entanto, a duplicação de regimes, originou incompatibilidades. Deste modo, este artigo tem como objetivo refletir sobre um ponto de colisão normativa referente à articulação entre o regime especial da Lei do Cibercrime e o regime geral do Código de Processo Penal, no que respeita à pesquisa de dados informáticos, consagrada no art.º 15.º da Lei do Cibercrime com remissão para o regime correspondente das buscas informáticas, previstas no art.º 174.º do Código de Processo Penal.

Palavras-Chave: Buscas Informáticas; Cibercrime; Pesquisa de Dados Informáticos; Prova Eletrónica.

Abstract

Cybercrime is a crime that crosses borders, and its prevalence has been increasing in recent years. Portugal, with the publication of the Cybercrime Law, now has, in addition to the Code of Criminal Procedure, another legal diploma aimed at preventing and combating computer crime, however, the duplication of regimes, led to incompatibilities. Thus, this article aims to reflect on a normative collision point regarding the articulation between the special regime of the Cybercrime Law and the general regime of the Code of Criminal Procedure, regarding the computer data research of, enshrined in article 15 of the Cybercrime Law with reference to the corresponding regime of computer data searches, provided for in article 174 of the Code of Criminal Procedure.

Keywords: Computer Data Research; Computer Data Search; Cybercrime; Electronic Evidence.

Introdução

As novas tecnologias possuem uma enorme relevância na vida dos cidadãos. Normalmente, são utilizadas em benefício dos seus utilizadores, permitindo que, em segundos, se possa ter acesso a informações contidas 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, 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.

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.

Tal como referem Holt e Bossler (2017), a emergência dos *smartphones* e computadores transformou o mundo e permitiu que os indivíduos se envolvessem, de diferentes formas, em crimes.

A prevalência criminal do facto aumentou, drasticamente, na última década. De acordo com a Procuradoria-Geral da República (2022), as denúncias de cibercrime têm vindo a aumentar, de uma forma consistente, desde o ano de 2016. No ano de 2020, 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.

Nas palavras de Venâncio (2022), a aplicabilidade do Direito Positivo à sociedade de informação levantou, desde sempre, diversos problemas de competência territorial, de ausência de previsão legal das suas tecnologias, de novos bens e serviços dificilmente enquadráveis nos institutos legais já existentes. Todos estes fatores, exponenciam os efeitos das tecnologias da informação enquanto fatores facilitadores da prática de atos ilícitos.

Pelo exposto, para promover o combate à cibercriminalidade, a Europa tem vindo a aprimorar a legislação e, em 2009, com a publicação da Lei n.º 109/2009 de 15 de setembro, a designada Lei do Cibercrime, Portugal transpôs para a ordem interna a Decisão-Quadro n.º 2005/222/JAI do Conselho da Europa.

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 bens jurídicos fundamentais.

Uma das principais formas de crime é, sem dúvida, o cibercrime que, conforme refere Rodrigues Nunes (2020), constitui, na atualidade, uma das principais ameaças ao respeito dos Direitos Fundamentais dos cidadãos, podendo até ser, por variadas razões, uma ameaça à segurança interna e internacional.

Procurando definir cibercriminalidade, podemos referir que, de acordo com a Comissão Europeia (2007)[1], 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. Melhor explica Rodrigues Nunes (2020) 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, entre outras, a disseminação de vírus, a falsidade informática, as invasões de sistema, a violação de dados pessoais ou o acesso a informações confidenciais.

Nas palavras de Marques Dias (2014) e Rodrigues Nunes (2020), a sistematização da cibercriminalidade pode ser entendida seguindo dois 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; (b) por outro lado, num sentido 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 subsumam, apenas e só, 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 do Cibercrime.

Para Venâncio (2022), criminalidade informática, em sentido estrito, é aquela em que o elemento digital ou informático surge como uma parte integrante do tipo legal ou mesmo como seu objeto de proteção. De outra forma, em sentido amplo, não só os que têm por bem jurídico protegido o próprio acesso ou funcionalidade da

[1] 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. Recuperado de https://eur-lex.europa.eu.

sociedade da informação, mas todos aqueles em que a informática é uma parte necessária dos seus elementos típicos, ou seja, o elemento digital ou informático é apenas um meio (entre outros) para a prático de um crime.

Tendo em conta a própria natureza do crime, a investigação sobre o cibercrime recorre a diligências de obtenção de prova em suporte eletrónico, o que implica que ocorra uma efetiva cooperação entre diversas entidades internacionais, porque, como se pode perceber, tendo em conta o âmbito global da cibercriminalidade, facilmente se perspetiva este tipo de crime como sendo delitos que ultrapassam 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 eficaz.

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 (2012), 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.

Na Europa, têm vindo a ser desenvolvidas diversas fontes normativas no que respeita à cibercriminalidade, dado que, com o acelerar do avanço tecnológico, são necessárias respostas eficazes e imediatas no combate a este tipo de crimes. Os principais diplomas internacionais que estiveram na base da atual Lei do Cibercrime são a Convenção sobre o Cibercrime do Conselho da Europa, a Decisão-Quadro do Conselho Europeu e a Diretiva do Parlamento Europeu e do Conselho Europeu e a Lei n.º 32/2008, de 17 de julho, os quais serão analisados em seguida.

A Convenção sobre o Cibercrime do Conselho da Europa, de 23 de novembro de 2001, aberta à assinatura em Budapeste[2], 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[3].

Para além da Convenção sobre o Cibercrime atrás referida, que serviu de paradigma para a elaboração Lei do Cibercrime, importa também destacar um outro diploma legal: a Decisão-Quadro n.º 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 e teve como fundamento 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 transfronteiriços contra os sistemas de informação, o que faz realçar a absoluta necessidade de harmonizar as legislações penais no âmbito da cibercriminalidade[4].

[2] Daí ser conhecida como Convenção de Budapeste, ratificada, atualmente, por alguns países da América Latina, dos quais se incluem o Brasil. Esta convenção é o tratado mais relevante e abrangente em matéria de cibercriminalidade.

[3] Portugal subscreveu a Convenção sobre o Cibercrime em 2001, no entanto, só procedeu à sua ratificação em 2009, por Resolução da Assembleia da República n.º 88/2009 e pelo Decreto do Presidente da República n.º 92/2009, ambos publicados a 15 de setembro, data que corresponde à publicação da Lei n.º 109/2009, de 15 de setembro. A Lei n.º 109/2009, de 15 de setembro, como consta no próprio texto, adaptou ao direito interno a Convenção sobre o Cibercrime.

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

A Diretiva n.º 2006/24/CE, do Parlamento e do Conselho, de 15 de julho[5], 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 n.º 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.

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 é, ainda hoje, considerada como o mais importante trabalho internacional versando a temática cibercrime. Em 2009, com a publicação da Lei do Cibercrime[6], o legislador nacional consagrou, finalmente, um autêntico sistema processual de prova em suporte eletrónico. Portugal transpôs, para a ordem interna, a Decisão-Quadro n.º 2005/222/JAI do Conselho da Europa, relativa a ataques contra sistemas de informação[7], respeitando as obrigações internacionais a que o Estado Português estava adstrito.

Recentemente, no ano de 2021, a Lei n.º 79/2021, de 24 de novembro, que transpõe a Diretiva 2019/713 do Parlamento Europeu e do Conselho da Europa, de 17 de abril de 2019, que é relativa ao combate à fraude e à contrafação de meios de pagamento efetuados não em numerário, veio alterar a legislação em Portugal, designadamente o Código Penal, o Código de Processo Penal e a Lei do Cibercrime[8].

Regime Jurídico da Prova Eletrónica

Passando, seguidamente, a analisar o regime jurídico da prova eletrónica, como ponto prévio, é importante realçar que a reflexão acerca do acesso e análise da prova, enquanto mecanismos de reconstrução da verdade material, sempre foram um tema imensamente debatido no domínio do Direito Processual Penal, não sendo alheio a este facto, o seu cariz pertinente, mas, ao mesmo tempo, controverso.

O regime legal da prova está codificado no livro III do Código de Processo Penal Português[9]. Embora uma parte deste livro seja dedicado a este tema, na verdade, o Direito Adjetivo não apresenta qualquer conceito de prova[10], limitando as suas referências unicamente ao seu objeto. Doutrinalmente, de acordo com Simas Santos & Leal-Henriques (2011), 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, pelo que podemos ver a prova como resultado ou a prova como demonstração.

Passando a refletir sobre o regime da sua admissibilidade, importa salientar que todas as provas são admissíveis, excetuando apenas aquelas que são proibidas pela lei (art.º 127.º do Código de Processo Penal Português e art.º 32.º/8 e 34.º/4 da Constituição da República Portuguesa). Do exposto, resulta o art.º 126.º/1 e 3 do Código de Processo Penal Português, mencionando que são nulas quaisquer provas obtidas mediante tortura, coação ou com ofensa da integridade física das pessoas, e, ressalvados os casos previstos na lei, são igualmente nulas, não

[5] 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.
[6] Revogando a Lei da Criminalidade Informática, Lei n.º 109/91 de 17 de agosto.
[7] Tal como refere o art.º 1.º da Lei n.º 109/2009 de 15 de setembro.
[8] Na Lei do Cibercrime foram alterados os art.º 3.º, 6.º, 19.º, 20.º, 21.º, 25.º e 30.º e aditados os art.º 3.º- A, 3.º- B, 3.º- C, 3.º- D, 3.º- F e 3.º- G. Estas alterações entraram em vigor em 24 de dezembro de 2021.
[9] O Código de Processo Penal Português, no art.º 124.º, menciona que 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.
[10] O Código Civil Português, no art.º 341.º, expressa uma definição mais específica de prova, referindo que as provas têm por função a demonstração da verdade 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.

podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações, sem o consentimento do respetivo titular[11].

No que concerne à atividade probatória, o Direito Processual Penal português estabelece a distinção entre os designados meios de prova e os meios de obtenção 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 (Simas Santos & Leal-Henriques, 2011).

Nos tempos hodiernos, um dos principais meios de obtenção de prova é, sem qualquer dúvida, a prova em suporte eletrónico. Em concordância total com este facto, refere Fidalgo (2019) que a prova eletrónica constitui o cerne da generalidade dos processos em matéria penal.

Procurando clarificar os conceitos, importa, desde já, mencionar que a prova eletrónica se diferencia da prova digital. Fidalgo (2019) esclarece estes preceitos, referindo que a primeira é um conceito mais amplo, dado que envolve, para além das provas em formato digital, as provas em formato analógico. A prova digital, como se percebe, apenas envolve dados em formato digital.

A prova em suporte eletrónico corresponde à informação passível de ser extraída de um dispositivo eletrónico ou de uma rede de comunicações. Porquanto, a prova eletrónica, para além de ser admissível, deve ser também fidedigna, explicita e consistente (Venâncio, 2022).

A valoração da prova em suporte eletrónico tornou-se num tema fundamental no combate à criminalidade informática não apenas em Portugal, mas também a nível internacional. Devido à sua natureza, apresenta caraterísticas que a diferenciam dos meios de obtenção de prova clássicos: (a) é uma prova de acesso complexo, dado que tem um 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, onde facilmente se escondem esses dados, podendo ser ocultados ou suprimidos do suporte original; e (d) é frágil, exigindo especiais cuidados no seu manuseamento, o que obriga, ao avaliador, conhecimentos técnicos e científicos elevados (Dias Ramos, 2014).

A complexidade da prova em suporte eletrónico surge, essencialmente, em 3 momentos distintos: a pesquisa, a obtenção de dados e a sua posterior conservação para uso em processo judicial no futuro (Venâncio, 2022). Quanto à pesquisa, este é um dos principais constrangimentos no acesso à prova eletrónica, dado que esta não remete necessariamente para o momento e para local da prática do crime, uma vez que ele pode ter sido cometido em qualquer parte do mundo. No que concerne à obtenção e conservação dos dados, existem também inúmeras dificuldades porque, na maioria dos casos, a prova para além de não se encontrar no local do crime, está na posse de terceiros.

Embora a doutrina reconheça, na atualidade, a enorme prevalência da prova eletrónica enquanto meio de obtenção de prova, até à entrada em vigor da Lei do Cibercrime, não existiam em Portugal regras especiais relativas à sua recolha[12]. Com a entrada em vigor da Lei do Cibercrime, a verdade é que continua a não ser inteiramente clara e objetiva a tutela da prova eletrónica no processo penal português. Tal como refere Conde Correia (2020), nesta matéria, Portugal continua a manter a sua regulação através de diplomas legais distintos, como sejam, o Código de Processo Penal e a Lei do Cibercrime, podendo ainda acrescentar a Lei relativa à

[11] Acórdão do Tribunal da Relação de Lisboa. Processo número 351/20.8PZLSB-C.L1-5, de 09 de novembro de 2021.
[12] A revogada Lei da Criminalidade Informática não estabelecia disposições de caráter processual.

Conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas, a Lei 32/2008 de 17 de julho.[13]

Concordando com as reflexões de Conde Correia (2020), este regime não uniforme, para além de prejudicar a centralidade normativa do Código de Processo Penal, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e prejudicial insucesso em termos práticos. Nas suas palavras, a prova eletrónica parece estar submersa num pântano lamacento de cariz normativo, que só poderá ser superado mediante uma intervenção legislativa doutrinalmente coerente.

Contudo, como realçado, a entrada em vigor da Lei do Cibercrime trouxe aspetos inovadores no que respeita à matéria da prova eletrónica, nomeadamente, o seu âmbito processual — previsto no art.º 11.º — o qual, ao procurar sistematizar a sua aplicabilidade, define também o círculo de aplicação das disposições processuais, onde se percebe que as normas aí previstas possuem uma extensão geral, uma vez que há a possibilidade de recorrer a estes meios de obtenção de prova para combate à criminalidade em geral, independentemente da forma.

De acordo com Venâncio (2023), defendendo o seu sentido amplo, a Lei do Cibercrime estabelece que as medidas relativas à preservação, revelação, apresentação, pesquisa e apreensão de dados informáticos destinam-se a todos os crimes que sejam cometidos por meio de um sistema informático e não apenas aos crimes informáticos aí previstos. Deste modo, estamos perante um regime processual de obtenção de prova eletrónica 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. O legislador, ao consagrar o regime especial da Lei do Cibercrime, aceitou outras formas de acesso a um sistema informático, pelo que a lei suprarreferida não possui o exclusivo na aquisição processual de dados informáticos[14].

Esta é também a ideia de Conde Correia (2020), ao acrescentar que a pesquisa de dados informáticos tem pressupostos e objetivos determinados e circunscritos que não prejudicam o regime geral. Todavia, embora doutrinalmente se reconheça que a Lei do Cibercrime sistematizou processualmente, e de uma forma não circunscrita, o regime de prova eletrónica (Conde Correia, 2020; Fidalgo, 2019; Venâncio, 2022), acabou por não o fazer de um modo muito claro, dado que veio produzir problemas na articulação com o Código de Processo Penal Português, porque o legislador, ao duplicar os regimes, consagrou as buscas no regime geral do Código de Processo Penal Português (art.º 174.º e 176.º) e a pesquisa de dados informáticos no regime especial da Lei do Cibercrime (art.º 15.º).

Analisando estes dois regimes, o regime geral das buscas e o regime especial da pesquisa de dados informáticos, importa salientar que, com o surgimento de novas formas de criminalidade cuja resposta eficaz depende em larga medida do recurso a meios de obtenção de prova mais diligentes, as buscas, tal como outros meios de obtenção de prova, vêm sendo relegadas para uma espécie de método oculto de investigação criminal, suscitando até algumas questões de possível violação constitucional.

As buscas são um meio de obtenção de prova que têm por objeto os locais e são ordenadas quando haja fundados indícios de que, em lugar reservado ou não livremente acessível ao público, se encontram objetos relacionados com um crime e que possam servir de prova (Rodrigues Nunes, 2019).

Verdelho (2009) e Silva Rodrigues (2011), com base no previsto no art.º 174.º/2 do Código de Processo Penal Português, em análise ao regime das buscas face à prova eletrónica, adaptam o conceito de buscas à realidade eletrónica, considerando que a busca informática é ordenada sempre que houver indícios de que alguém oculta

[13] Esta lei transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

[14] Os art.º 16.º e 17.º da Lei do Cibercrime consagram a possibilidade da ocorrerem "pesquisas informáticas ou outras formas de acesso legítimo a um sistema informático".

no seu computador, vestígios de crime informático que cometeu ou facilitou, de qualquer forma, o seu cometimento.

As pesquisas de dados informáticos, consagradas no art.º 15.º da Lei do Cibercrime, correspondem à expressão adotada na lei, para o que se poderia também designar de buscas informáticas. Refere 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, a pesquisa de tais dados no sistema informático, devendo, sempre que possível, presidir à diligência[15]. As medidas previstas neste artigo transpõem para o Direito português o regime processual previsto no art.º 19.º da Convenção de Budapeste, relativo à busca e apreensão de dados informáticos armazenados, que consiste nos procedimentos processuais adequados a validar a pesquisa de dados informáticos em sistemas informáticos suspeitos de conter informação necessária para a produção de prova, tendo em vista a descoberta da verdade (Venâncio, 2023).

Em comparação com as buscas tradicionais, as pesquisas de dados informáticos, devido à sua enorme intensidade intrusiva, apresentam características inovadoras e independentes (Conde Correia, 2020), as quais a Convenção de Budapeste procurou apontar.

A minuta do Relatório Explicativo da Convenção de Budapeste, no seu ponto 184, indica a necessidade de modernização e harmonização das legislações nacionais relativamente às buscas e apreensão de dados informáticos armazenados para fins de obtenção de provas relacionadas com investigações criminais, uma vez que, embora as diferentes legislações contemplem as buscas e as apreensões de objetos tangíveis, uma parte dos objetos de investigação não são algo tangível ou corpóreo[16]. No seu ponto 187, alerta-se ainda que, no que se refere à investigação de dados informatizados, são necessárias disposições complementares, com o intuito de assegurar que os dados informatizados possam ser obtidos com o mesmo grau de eficácia de uma operação de busca e apreensão em suportes tangíveis.

Pelo exposto, em decorrência da norma do art.º 15.º/6 da Lei do Cibercrime, consideramos que se aplica às pesquisas de dados informáticos, com as necessárias adaptações, as regras das execuções das buscas previstas no Código de Processo Penal Português, especificamente nos art.º 174.º e 251.º, as quais são autorizadas ou ordenadas por despacho de uma autoridade judiciária competente[17], devendo esta, sempre que seja possível, presidir à diligência. Em regra, é ao Ministério Público (na fase de inquérito), ao juiz de instrução criminal (na fase de instrução) e ao juiz (na fase de julgamento), que são as autoridades judiciárias competentes, que autorizam ou ordenam a realização de pesquisas de dados informáticos.

Num acórdão do Tribunal da Relação de Évora[18], ressalta-se que os dados, preservados ou conservados em sistemas informáticos, só podem ser acedidos, em inquérito, através de injunção do Ministério Público ou por decisão do Juiz de Instrução. Num acórdão do Tribunal da Relação do Porto[19], refere-se que, tendo a prova sido obtida pela Polícia Judiciária, sem despacho prévio de um Magistrado do Ministério Público, sem que haja uma decisão prévia do Juiz de Instrução, esta deve ser considerada como inválida.

---

[15] Para além da situação referida, as pesquisas de dados informáticos, estão também previstas para situações em que surjam razões, durante a pesquisa, para acreditar que os dados procurados se podem encontrar num sistema informático diferente e que podem ser acessíveis através do sistema inicial, estendendo essa mesma pesquisa mediante autorização da entidade competente.

[16] Conselho da Europa. Minuta em português do Relatório Explicativo da Convenção sobre o Cibercrime, de 23.11.2001. https://rm.coe.int/16802fa429.

[17] A decisão da autoridade judiciária de realização de pesquisa de dados em suporte eletrónico tem um prazo de validade de 30 dias.

[18] Acórdão do Tribunal da Relação de Évora, de 02 de maio de 2017. Processo número 445/10.8JAFAR.

[19] Acórdão do Tribunal da Relação do Porto, de 22 de maio de 2013. Processo número 74/07.3PASTS.P1.

No art.º 15.º/3 a) da Lei do Cibercrime, está previsto um regime de salvaguarda, onde se estabelece que o órgão de polícia criminal pode proceder à pesquisa sem que haja prévia autorização da autoridade judiciária, no caso, por exemplo, quando a mesma for voluntariamente consentida por quem tiver a disponibilidade ou o controlo desses mesmos dados. Por outro lado, o Código de Processo Penal, no art.º 174.º/5 b), permite que o órgão de polícia criminal efetue buscas sem que haja autorização prévia da autoridade judiciária, nas situações em que os visados consintam.

Refletindo acerca do texto da lei, percebe-se que, em rigor, se denotam incompatibilidades entre o regime geral do Código de Processo Penal Português e o regime especial da Lei do Cibercrime, designadamente na articulação entre os art.º 174.º/5 b) do Código de Processo Penal e art.º 15.º/3 a) da Lei do Cibercrime.

Imagine-se a situação em que aquele que possui a disponibilidade e o controlo dos dados (cf. Lei do Cibercrime) pode não ser o visado (cf. Código de Processo Penal), originado que quem tem a disponibilidade e o controlo manifesta consentimento para a pesquisa de dados eletrónicos, no entanto, o visado não consente.

Como deve proceder a autoridade judiciária quando for realizada uma pesquisa a dados armazenados em suporte eletrónico numa determinada empresa, na qual essa mesma empresa detém e fornece o consentimento para a pesquisa dos dados, no entanto, o visado não fornece o consentimento para a sua realização?

De acordo com Rodrigues Nunes (2018), as pessoas que têm a posse física dos dados, ou que não a tendo, podem legitimamente aceder-lhes, mesmo se não forem visados pela investigação, bastará o consentimento de uma delas.

É neste sentido que somos levados a concordar com a interpretação de Conde Correia (2020), que considera que quando se trata de uma empresa e não de um computador pessoal, em princípio, o órgão de gestão dessa mesma empresa pode permitir o acesso aos dados do computador pelos órgãos de polícia criminal, sem que haja a necessidade de um despacho prévio de autorização por parte de uma autoridade judiciária ou do consentimento do visado, desde que haja consentimento dos órgãos de gestão, detentor do controlo dos dados em questão e que esse consentimento fique, por qualquer forma, documentado.

O consentimento assume-se como um pressuposto de validade da diligência, observando-se o estipulado no art.º 38.º/2 do Código Penal Português que refere que o consentimento pode ser expresso por qualquer meio que traduza uma vontade séria, livre e esclarecida do titular do interesse juridicamente protegido e pode ser livremente revogado até à execução do facto.

Considerações Finais

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 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 em suporte eletrónico, a Lei do Cibercrime veio superar uma lacuna que existia no ordenamento jurídico-penal em Portugal. No entanto, como não originou uma revogação expressa do Código de Processo Penal Português, 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 Lei do Cibercrime, em detrimento do regime geral do Código de Processo Penal Português.

Em nosso entender, percebe-se que o legislador, ao consagrar o regime da prova eletrónica na Lei do Cibercrime, pretende fornecer aos órgãos de polícia criminal instrumentos de combate à criminalidade em geral, pelo que nos parece ser incorreto encontrar, na norma da Lei do Cibercrime referente à pesquisa de dados informáticos, alguma forma de substituição para o consagrado no Código de Processo Penal Português para esta matéria, uma

vez que a própria Lei do Cibercrime reconhece a possibilidade de aplicação de outras leis, distanciando-se, assim, da exclusividade de aplicação.

A Lei do Cibercrime apresenta um regime geral de recolha de prova em suporte eletrónico, que é aplicável a qualquer processo criminal. Por isso, as normas desta lei deveriam ter tido um enquadramento sistemático no Código de Processo Penal português, de modo a evitar dificuldades na harmonização da lei com o código.

Referências Bibliográficas

Coelho dos Santos, R. (2005). O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos. *Boletim da Faculdade de Direito*. Coimbra Editora.

Comissão Europeia (2007). Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões. *Rumo a uma política geral de luta contra o cibercrime*. https://eur-lex.europa.eu

Conde Correia, J. (2014). Prova digital: as leis que temos e a lei que deveríamos ter. *Revista do Ministério Público*, *139*, 29–59.

Conde Correia, J. (2020). Prova digital: enquadramento legal. *Cibercriminalidade e prova digital. Jurisdição penal e processual penal*, 23–37. Centro de Estudos Judiciários.

Dias Ramos, A. (2014). *A prova digital em Processo Penal*. Chiado Editora.

Fidalgo, S. (2019). A recolha de prova em suporte eletrónico — em particular, a apreensão de correio eletrónico. *Revista Julgar*, *38*, 151–160.

Holt, T. J. & Bossler, A. M. (2017). *Cybercrime in Progress. Theory and prevention of technologyenabled offenses*. Taylor & Francis.

Lopes Militão, R. (2012). A propósito da prova digital no processo penal. In *Revista da Ordem dos Advogados*, *72*(5), 247–285.

Marques da Silva, G. (2010). *Curso de Processo Penal — noções gerais, elementos do processo penal* (vol. I). Verbo Editora.

Marques Dias, V. (2012). A problemática da investigação do cibercrime. *Data Venia, Revista Jurídica Digital*, *1*(1), 63–88.

Procuradoria-Geral da República. (2022). *Cibercrime: denúncias recebidas*. Ministério Público de Portugal.

Ramalho, J. (2022). Prova digital: articulação entre o Código Processual Penal Português e a Lei do Cibercrime. *Revista Eletrónica Direito Penal e Política Criminal*, *10*(2), pp. 7–20.

Rodrigues Nunes, D. (2018). *Os meios de obtenção de prova previstos na lei do cibercrime*. Editora Gestlegal.

Rodrigues Nunes, D. (2019). *Revistas e Buscas no Código de Processo Penal*. Editora Gestlegal.

Rodrigues Nunes, D. (2020). *Os crimes previstos na lei do cibercrime*. Editora Gestlegal.

Silva Rodrigues, B. (2011). *Da Prova Penal* (tomo IV). Rei dos Livros.

Simas Santos, M. & Leal-Henriques, M. (2011). *Noções de Direito Processual Penal.* Editora Rei dos Livros.

Venâncio, P. D. (2022). *Lições de Direito do Cibercrime. E da tutela penal dos dados pessoais*. Editora D'Ideias.

Venâncio, P. D. (2023). *Lei do Cibercrime: anotada e comentada*. Editora D'Ideias.

Verdelho, P. (2009). *A nova lei do Cibercrime* (tomo LVIII). Scientia Juridica.

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla revisão anónima por pares.