Revista JURÍDICA PORTUCALENSE

www.upt.pt

UNIVERSIDADE PORTUCALENSE
IJP Instituto Jurídico Portucalense

Fundação para a Ciência e a Tecnologia

Nº 35 | Universidade Portucalense | Porto | 2024

https://doi.org/10.34625/issn.2183-2705(35)2024

Joaquim RAMALHO, Fernando ALMEIDA

Apreensão de Correio Eletrónico: Os Regimes do Código de Processo Penal e da Lei do Cibercrime

DOI: https://doi.org/10.34625/issn.2183-2705(35)2024.ic-13

Secção I

Investigação Científica*

* Os artigos presentes nesta secção foram sujeitos a processo de revisão segundo o método *blind peer review* / The articles in this section have undergone a blind peer review process.

Apreensão de Correio Eletrónico: Os Regimes do Código de Processo Penal e da Lei do Cibercrime

Apprehend Electronic Mail: The Code of Criminal Procedure and Cybercrime Law Regimes

Joaquim RAMALHO[1]
Fernando ALMEIDA[2]

RESUMO: O cibercrime é um tipo de crime cuja prevalência tem vindo aumentar de uma forma considerável ao longo dos últimos anos. A publicação da Lei do Cibercrime procurou prevenir e combater a criminalidade informática, contudo a duplicação de regimes com o Código de Processo Penal originou dificuldades na sua interconexão entre as normas. Deste modo, este trabalho visa refletir sobre o processo do regime especial de apreensão de correio eletrónico e o regime geral da apreensão de correspondência, quanto à necessidade de despacho prévio do juiz para que seja efetuada a respetiva apreensão.
PALAVRAS-CHAVE: Cibercrime; Convenção de Budapeste; Prova Eletrónica; Apreensão de Correio Eletrónico; Apreensão de Correspondência

ABSTRACT: Cybercrime is a crime whose prevalence has increased considerably over recent years. The publication of the Cybercrime Law sought to prevent and combat computer crime, however the duplication of regimes with the Code of Criminal Procedure led to difficulties in their interconnection between the norms. Therefore, this paper aims to reflect on the process of the special regime for the apprehend of electronic mail and the general regime for the correspondence apprehend, regarding the need for a prior order from the judge for the respective apprehension.
KEYWORDS: Cybercrime; Budapest Convention; Eletronic support evidence; Apprehend Electronic Mail; Correspondence Apprehend.

[1] Advogado; Licenciado em Direito pela Faculdade de Direito da Universidade do Porto; Mestre em Direito pela Faculdade de Direito da Universidade do Porto; Doutor em Direito pela Faculdad de Ciencias Jurídicas y del Trabajo, Universidad de Vigo, Espanha; Professor Associado na Faculdade de Ciências Humanas e Sociais, Universidade Fernando Pessoa; Investigador no Observatório Permanente de Violência e Crime, Universidade Fernando Pessoa; Investigador no FP-B2S da Universidade Fernando Pessoa; ORCID: https://orcid.org/0000-0002-1105-9740; E-mail: ramalho@ufp.edu.pt.
[2] Licenciado em Economia pela Faculdade de Economia da Universidade do Porto; Licenciado em Direito pela Faculdade de Direito da Universidade do Porto; Doutor em Economia pela Universidade de Santiago de Compostela, Espanha; Professor Catedrático Jubilado da Universidade Lusíada, Porto; Antigo Diretor da Faculdade de Ciências Empresariais da Universidade Lusíada, Porto; Investigador no Centro de Estudos da População Economia e Sociedade da Universidade do Porto; ORCID: https://orcid.org/0000-0002-6430-3591.

1. Introdução

A forma de contacto entre os seres humanos, em consequência da revolução tecnológica e da globalização, tem vindo a ser modificada, dando origem a novas formas relacionais. Com as novas tecnologias, o ciberespaço, através do qual é dispensável a presença física para que se possa estabelecer uma comunicação relacional, ganhou preponderância, ao funcionar como um espaço de partilha de informações e de contacto entre pessoas de diversas as partes do mundo.

Normalmente, as novas tecnologias são utilizadas em benefício dos próprios utilizadores, permitindo que, em segundos, se possa ter acesso a informação contida em qualquer parte do mundo, todavia, estas não acarretam apenas vantagens. A utilização universal do correio eletrónico ou das redes sociais, entre outras, constituem um incentivo à proliferação de determinados tipos de criminalidade, nomeadamente os que são perpetrados com recurso às tecnologias.

O índice de prevalência criminal relativa à cibercriminalidade, nas suas diferentes facetas, tem vindo a aumentar de uma forma significativa nos últimos anos. Estes dados são comprovados pela Procuradoria-Geral da República[3], verificando-se que as denúncias de cibercrime têm vindo a aumentar, de uma forma consistente desde o ano de 2016. Contudo, após o ano de 2020, as denúncias quase duplicaram, não sendo alheio, certamente, o confinamento das pessoas em resultado da situação pandémica vivida.

Atendendo à própria natureza e configuração do crime, será de admitir que a prevalência criminal dos factos ocorridos poderá ser ainda bastante superior ao número de denúncias. Urge, assim, criar institutos legais eficazes e enquadráveis nos já existentes, uma vez que a aplicabilidade do direito positivo às novas tecnologias, levantou, desde sempre, diversos problemas de competência territorial e de ausência de previsão legal para a tutela de novos bens jurídicos.

Em Portugal, com a promulgação de diplomas legais destinados a combater o cibercrime, procura-se prevenir a sua prática, no entanto, a conexão

[3] PROCURADORIA-GERAL DA REPÚBLICA, *Cibercrime: relatório de denúncias recebidas*, Ministério Público de Portugal, 2022.

entre regimes legais, como sejam o regime especial da Lei do Cibercrime e o regime geral do Código de Processo Penal, tem promovido discussão doutrinal e jurisprudencial, nomeadamente nas normas previstas no regime especial que remetem para o regime geral.

Tendo em conta o suprarreferido, esta investigação tem como principal objetivo proporcional uma reflexão acerca da divergência doutrinal existente entre, por um lado, a que realça a necessidade de despacho prévio do juiz de instrução para apreensão de correio eletrónico e, por outro, a que admite que, de uma forma cautelar, os órgãos de polícia criminal, tendo até em conta o interesse no desenvolvimento da investigação, possam fazer uma apreensão provisória da mesma, sem que haja despacho prévio da entidade judicial.

2. Cibercrime e acesso à prova eletrónica

O cibercrime, devido à sua natureza transfronteiriça e ao impacto que apresenta na sociedade contemporânea, constitui uma das principais ameaças à segurança interna e internacional, tendo simultaneamente um impacto significativo na concretização e na tutela dos direitos, liberdades e garantias, constitucionalmente previstos.

Fazendo um breve enquadramento conceptual, a Comissão Europeia[4] considera que o cibercrime corresponde aos atos criminosos praticados com recurso ou contra as redes comunicacionais eletrónicas e sistemas de informação. Melhor explica Rodrigues Nunes[5], acrescentando que o cibercrime encerra na designação dada aos crimes cibernéticos que envolvem qualquer tipo de atividade ou de prática ilícita na rede, como sejam disseminação de vírus, falsidade informática, invasões de sistema, violação de dados pessoais ou acesso a informações confidenciais.

Procurando delimitar o conceito de cibercrime, postula Dias Venâncio[6] que a sistematização da cibercriminalidade pode ser entendida por duas perspetivas distintas: (a) em sentido estrito - aquela em que o elemento

[4] 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, 2007.
[5] RODRIGUES NUNES, Duarte. *Os crimes previstos na lei do cibercrime, Coimbra*, Editora Gestlegal, 2020.
[6] DIAS VENÂNCIO, Pedro. *Lições de Direito do Cibercrime, E da tutela penal dos dados pessoais*, Coimbra, Editora D´Ideias, 2022.

informático é enquadrado num elemento integrante do tipo legal ou como bem jurídico a proteger; (b) em sentido amplo - aquela em que não só os que têm por bem jurídico protegido o próprio acesso ou a funcionalidade da sociedade da informação, mas também todos aqueles em que a informática é uma parte necessária dos seus elementos típicos, ou seja, em que o elemento informático é apenas um meio que serve de facilitador da prática de um determinado crime.

Percebendo a natureza global deste crime, a inquirição dos cibercrimes necessita de uma efetiva cooperação entre as diversas entidades internacionais. Em resultado desta necessidade, diversos legisladores no mundo e particularmente na europa, têm vindo a desenvolver diversas fontes normativas que promovam o seu combate.

Até ao ano de 2009, Portugal não havia dado cumprimento aos diferentes preceitos de cariz internacional a que se encontrava vinculado, por ter assinado, em 23 de novembro de 2001, a Convenção sobre o Cibercrime do Conselho da Europa[7], que é, ainda hoje, considerado como o primeiro e mais importante trabalho internacional sobre o cibercrime. Reconhecendo a ordem jurídica portuguesa a inadequação à nova realidade criminal, nesse mesmo ano, com a publicação da Lei do Cibercrime[8], o legislador consagrou, finalmente, um diploma substantivo e adjetivo de prova em suporte eletrónico, ao transpor, para a ordem interna, a Decisão-Quadro número 2005/222/JAI do Conselho da Europa, relativa a ataques contra sistemas de informação, fazendo respeitar as obrigações internacionais a que estava vinculado.

A Lei do Cibercrime, embora seja inovadora no que respeita ao regime da prova, nomeadamente quanto aos meios de obtenção de prova, é também neste regime que tem vindo a surgir maior controvérsia, originando enorme discussão doutrinal, não só pelas dificuldades de interconexão do regime especial da Lei do Cibercrime com o regime geral do Código de Processo Penal, mas ainda pelo facto desta matéria estar regulada em legislação avulsa.

Uma das principais controvérsias está presente numa matéria que constitui um dos mecanismos mais relevantes de reconstrução da verdade

[7] In https://rm.coe.int/16802fa428
[8] LEI DO CIBERCRIME. Lei número 109/2009 de 15 de setembro. Diário da República série I de 15.09.2009.

material, que é o regime de acesso e de apreensão de prova eletrónica, o qual merecerá, da nossa parte, uma cogitação mais exaustiva infra.

O regime geral da prova está previsto no livro III do Código de Processo Penal. Embora parte deste livro seja dedicado ao tema, na verdade, o direito adjetivo não apresenta qualquer conceito de prova, limitando as suas referências unicamente ao seu objeto.

O Código Civil, no seu artigo 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.

Doutrinalmente, entende-se a prova como correspondendo à atividade que se destina a demonstrar a verdade dos factos ocorridos[9], ou seja, é um processo 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[10].

Na atualidade, um dos principais meios de obtenção de prova é a prova em suporte eletrónico, constituindo esta o núcleo dos processos em matéria penal.

Procurando clarificar o conceito, importa, desde já, mencionar que a prova eletrónica se diferencia da designada prova digital. Fidalgo[11], 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, é um conceito mais restrito, uma vez que apenas é respeitante a 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 e, tendo em consideração o crescimento exponencial da desmaterialização dos processos, a sua valoração tornou-se um tema fundamental no combate à

[9] COSTA ANDRADE, Manuel. *Sobre as proibições de prova em processo penal*, Coimbra, Editora Gestlegal, 2ª edição, 2022.
[10] SIMAS-SANTOS; Manuel; LEAL-HENRIQUES, Manuel; SIMAS-SANTOS, João. *Noções de Processo Penal*, 3ª edição, Lisboa, Rei dos Livros, 2020.
[11] FIDALGO, Sónia. A recolha de prova em suporte eletrónico - em particular a apreensão de correio eletrónico, *Revista Julgar*, *38*, pp. 151-160, 2019.

criminalidade informática, não apenas em Portugal, mas também a nível internacional.

Devido à sua natureza, a prova em suporte eletrónico possui uma natureza diferenciadora quando comparada com outros meios de obtenção de prova, *verbi gratia*, devido ao seu caráter temporário, à sua fungibilidade e volatilidade em consequência da sua natureza imaterial[12]. Porquanto, de forma a procurar suprir os constrangimentos suprarreferidos, a prova eletrónica, nas palavras de Dias Venâncio[13], terá de ser também admissível, fidedigna, explícita e consistente, uma vez que, devido a toda a sua especificidade, ela possui uma natureza extremamente complexa, que surge em 3 momentos distintos: a pesquisa, a obtenção de dados e a sua posterior conservação para uso em processo judicial futuro.

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, resultam também daqui inúmeras dificuldades uma vez que, na maioria dos casos, a prova para além de não se encontrar no local do crime, pode estar na posse de terceiros e o seu acesso envolve uma definição concreta.

Embora a doutrina reconheça, na atualidade, a enorme prevalência da prova eletrónica enquanto meio de obtenção de prova, a verdade é que até ao momento da entrada em vigor da Lei do Cibercrime, não existiam em Portugal regras especiais relativas à sua recolha, uma vez que a investigação da criminalidade informática era feita através do recurso às regras gerais do Código de Processo Penal porque a revogada Lei da Criminalidade Informática não estabelecia disposições de caráter processual. Com a sua promulgação, a verdade é que continua a não ser inteiramente clara e objetiva a tutela da prova eletrónica no processo penal português, porque continua a manter-se a sua

[12] DIAS RAMOS, Armando. *A prova digital em Processo Penal*, Lisboa, Chiado Editora, 2014.
[13] DIAS VENÂNCIO, Pedro. *Lições de Direito do Cibercrime, E da tutela penal dos dados pessoais*, Coimbra, Editora D´Ideias, 2022.

regulação através de, pelo menos, dois diplomas legais distintos - o Código de Processo Penal e a Lei do Cibercrime[14].

Com base no suprarreferido, o regime jurídico da prova eletrónica, devido à falta de centralidade normativa, tem vindo a potenciar dificuldades de conexão normativa, dado que, embora - como anteriormente realçado - a entrada em vigor da Lei do Cibercrime, acarrete aspetos inovadores à matéria da prova eletrónica, nomeadamente, o seu âmbito processual, ao procurar sistematizar a sua aplicabilidade, a Lei do Cibercrime define também um círculo de aplicação no qual 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.

A norma constante do artigo 11.º apresenta um âmbito de aplicação amplo, não se limitando aos crimes nela consagrados. Conforme o disposto na aliena c), as suas disposições são aplicáveis a todo e qualquer crime, desde que seja necessária a recolha de prova em suporte eletrónico, ou seja, os meios de obtenção de prova podem ser todos aplicados, em qualquer crime realizado com suporte eletrónico.

É exatamente este o sentido de um acórdão recente do Tribunal Constitucional[15], de onde se transcreve "*a argumentação que se baseie na conceção de que as normas adjetivas presentes na Lei do Cibercrime possuem uma natureza excecional, não é procedente"*. Neste mesmo sentido, Dias Venâncio[16], defendendo o seu sentido amplo, salienta que 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*".

Pelo suprarreferido, defendendo a perspetiva ampla, somos levados a concordar que estamos perante um regime processual de obtenção de prova eletrónica com um âmbito de aplicação superior à própria Lei do Cibercrime, uma

[14] Poderíamos ainda acrescentar a Lei número 32/2008 de 17 de julho relativa à conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas, a qual transpõe para a ordem jurídica interna, a Diretiva número 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março.

[15] TRIBUNAL CONSTITUCIONAL. Processo número 687 de 29 de julho de 2021.

[16] DIAS VENÂNCIO, Pedro. *Lições de Direito do Cibercrime, E da tutela penal dos dados pessoais*, Coimbra, Editora D´Ideias, 2022, p. 21.

vez que esta, por interpretação extensiva, não restringe a sua aplicação aos processos relativos aos crimes que aí estão contemplados.

O legislador ao consagrar o regime especial da Lei do Cibercrime, aceitou claramente outras formas de acesso a um sistema informático, conforme plasmado na lei. Esta é também a consideração de Conde Correia[17], 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, tal como defendem, entre outros, Fidalgo e Dias Venâncio, o legislador acabou por não o fazer de uma forma absolutamente clara em certos regimes, designadamente naqueles em que a Lei do Cibercrime remete para o regime correspondente do Código de Processo Penal, como é o caso da apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17.º da Lei do Cibercrime), cuja remissão é feita para a apreensão de correspondência (artigo 179.º do Código de Processo Penal), os quais serão analisados, com mais pormenor, infra.

3. Apreensão de correio eletrónico

Ao longo dos últimos anos, a tradicional carta tem vindo a ser praticamente substituída pelo correio eletrónico e pelas comunicações de natureza semelhante, os quais possuem especificidades técnico-jurídicas que em pouco se assemelham às comunicações tradicionais. Porquanto, sendo cada vez mais prevalente a sua utilização, as mensagens que são encontradas e apreendidas em sistemas informáticos, constituem um meio determinante na obtenção de prova em processo penal, cuja tutela constitucional - a direitos marcadamente individuais – tem, igualmente, merecido um interesse amplo na salvaguarda de direitos fundamentais, como o direito à reserva e intimidade da vida privada (artigo 26.º) e o direito à inviolabilidade de correspondência (artigo 34.º).

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

Decorrente da sua elevada pertinência, mas também atualidade, o regime jurídico do correio eletrónico e registos de comunicações de natureza semelhante correspondeu a uma das principais inovações presentes aquando da promulgação da Lei do Cibercrime.

O regime geral de apreensão de dados informáticos encontra-se plasmado no artigo 16.º números 1 e 2, enquanto o regime especial, por sua vez, encontra-se previsto no artigo 16.º números 3, 5 e 6 e no artigo 17.º da Lei do Cibercrime[18].

O regime jurídico do correio eletrónico e registos de comunicações de natureza semelhante, previsto seu artigo 17.º, correspondeu a uma das principais inovações presentes aquando da promulgação da Lei do Cibercrime. É um produto do legislador nacional e não resulta de qualquer fonte europeia. Deste modo, não havendo, na sua génese, uma referência normativa internacional, a sua interpretação tem vindo a gerar controvérsia.

Começando por refletir sobre a própria letra da lei, refere o artigo que quando

> "*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*"[19].

[18] Para acesso aos dados, estabelece o artigo 14.º da Lei do Cibercrime, respeitante à "*Injunção para apresentação ou concessão de acesso a dados*", que se "*no decurso do processo se tornar necessário à produção de prova (…) obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena, a quem tenha disponibilidade ou controlo desses dados, que os comunique ao processo ou que permita o acesso aos mesmos*". No artigo 15.º, que respeita às "pesquisas de dados informáticos", refere a 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, a pesquisa de tais dados no sistema informático, devendo, sempre que possível, presidir à diligência*". Quanto ao regime da "*apreensão de dados informáticos*", estabelece o artigo 16.º, que se "*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 (…), a autoridade judiciária competente autoriza ou ordena, por despacho, a apreensão dos mesmos*".

[19] O artigo 17.º da Lei do Cibercrime não tem previsão sobre a apreensão de correspondência eletrónica ou de natureza semelhante entre o arguido e o seu defensor, pelo que deve operar a

Levando em conta o texto normativo, é, desde logo, necessário perceber qual o seu âmbito de aplicação. Concordando com Dias Venâncio[20], devem entender-se abrangidos por esta apreensão unicamente os dados de conteúdos das mensagens de correio eletrónico ou os registos de comunicações de natureza semelhante, sendo excluídos, por exemplo, os dados de tráfego relativos à respetiva comunicação. Quanto à delimitação das comunicações de natureza semelhante, conforme refere um acórdão do Tribunal da Relação de Lisboa[21], estas também podem ser realizadas por telefone (em que a pessoa está identificada pelo seu número de telefone) ou através da internet (na qual se identifica a pessoa pela atribuição de um endereço de IP).

É no regime especial da apreensão de correio eletrónico, que a doutrina e a jurisprudência têm encontrado mais dificuldades na compatibilização com o regime geral relativo à apreensão de correspondência (artigo 179.º do Código de Processo Penal), uma vez que a norma prevista no artigo 17.º da Lei do Cibercrime, *in fine*, remete, correspondentemente, para o regime da apreensão de correspondência previsto no Código de Processo Penal.

Um primeiro problema surge no âmbito da possível necessidade, para que possa ocorrer uma apreensão formal do correio eletrónico, de existência de um despacho prévio do juiz de instrução que ordene ou autorize essa mesma apreensão.

Entendem Verdelho[22] e Cardoso[23] que, não sendo a lei objetiva nesta matéria, é possível ser realizada uma espécie de apreensão de cariz cautelar das mensagens de correio eletrónico - ainda que não exista o despacho prévio do juiz - sendo, posteriormente, possível juntar as mensagens ao processo se assim for determinado pelo juiz. Na hipótese de o juiz não autorizar essa mesma apreensão, a apreensão deverá ser concluída e as cópias que forem realizadas deverão ser destruídas.

---

remissão para o Código de Processo Penal, uma vez que, esta apenas será admissível se o juiz tiver fundadas razões para crer que aquela constitui objeto ou elemento de um crime.

[20] DIAS VENÂNCIO, Pedro. *Lei do Cibercrime: anotada e comentada*, Coimbra, Editora D´Ideias, 2023.

[21] TRIBUNAL DA RELAÇÃO DE LISBOA. Processo número 18/19.0YUSTR-N.L1-PICRS de 20 de fevereiro de 2023.

[22] VERDELHO, Pedro. *A nova lei do Cibercrime*, Tomo LVIII, Braga, Scientia Jurídica, 2009.

[23] 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*, *153*, pp. 167-214, 2018.

Esta interpretação da norma, na verdade, parece pretender operacionalizar a *praxis* da apreensão de correspondência, contudo, somos levados a discordar da interpretação suprarreferida, uma vez que não havendo esse despacho judicial prévio, não poderá ocorrer uma apreensão cautelar à espera do despacho.

Através da Interpretação da norma do artigo 17.º da Lei do Cibercrime, as mensagens de correio eletrónico ou de natureza semelhante não podem ser formalmente apreendidas, sem que haja um despacho prévio do juiz nesse sentido. É neste sentido, que vai o artigo 179.º número 1 do Código de Processo Penal. Aqui, refere-se que:

> "*sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que a correspondência foi expedida pelo suspeito ou lhe é dirigida*"[24]. Acrescenta o número 3 do mesmo artigo que "*o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ela ser utilizada como meio de prova*".

Parece-nos claro que o regime da apreensão de correio eletrónico é de competência exclusiva do juiz de instrução, uma vez que é apenas este que é competente para autorizar ou ordenar, por despacho, a apreensão, constituindo a mesma um meio de obtenção de prova admissível para crimes puníveis com pena de prisão de superior máximo a 3 anos.

Para a apreensão, os órgãos de polícia criminal transmitem a correspondência intacta ao juiz que autorizou ou ordenou a diligência, sendo este a primeira pessoa a tomar conhecimento do seu conteúdo. Se considerar relevante para a prova, deverá juntá-la ao processo, caso contrário, deverá restituí-la a quem de direito e sendo considerada como inválida.

Interpretando o espírito da norma, parece claro que a Lei do Cibercrime, ao remeter para o Código de Processo Penal não reduz o seu âmbito de aplicação, uma vez que faz sentido a aplicação literal correspondente da norma do artigo 179.º do Código de Processo Penal à apreensão de correio eletrónico, impondo aplicação da norma na sua totalidade. Neste mesmo sentido, vai o

[24] Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos e a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova.

recente acórdão do Tribunal da Relação de Lisboa[25] que considerou que a Lei do Cibercrime remete expressamente para o regime geral previsto no Código de Processo Penal, sem qualquer tipo de redução do seu âmbito. A remissão para o regime de apreensão da correspondência do Código de Processo Penal respeita também ao facto de ter de ser o juiz - que tiver autorizado ou ordenado a diligência - a primeira pessoa a tomar conhecimento do conteúdo do correio eletrónico e demais registos de comunicações apreendidos, mandando-os juntar ao processo se os considerar relevantes, sob pena de nulidade.

Conforme refere a jurisprudência, o Tribunal da Relação de Lisboa[26] considera que na apreensão de correio eletrónico, em processo penal, deve "aplicar-se o artigo 17.º da Lei do Cibercrime, tudo se processando como se de uma apreensão de correspondência, nos termos do Código de Processo Penal, se tratasse sendo, *ab initio*, necessária a autorização judicial para o efeito (…) Se assim for, a correspondência apreendida terá, obrigatoriamente, de ser presente e selecionada por um juiz antes de ser junta ao processo e poder aí ser considerada".

Neste mesmo sentido, vai um outro acórdão do Tribunal da Relação de Lisboa[27], onde é referido que

> "encontrando-se investigação em curso na fase de inquérito, a apreensão de correio eletrónico carece sempre de despacho judicial a autorizá-la nos termos do disposto nos artigos 17.º da Lei do Cibercrime e 179.º do Código de Processo Penal (...) e ambos os artigos sancionam com nulidade a violação das regras relativas à competência para a sua apreensão, uma vez que tal se justifica pelo princípio da proporcionalidade face ao especial dano social que implica a intromissão nos dados".

A própria Constituição da República Portuguesa, no artigo 20.º números 1, 4 e 5, artigo 32.º número 4 e artigo 202.º número 2, releva a intervenção de um juiz de instrução criminal como traduzindo um direito fundamental, para efeitos de autorização ou determinação da prática de atos de investigação, no decurso da fase de inquérito, que se assumam como relevantemente passíveis de colidir com outros direitos fundamentais.

[25] TRIBUNAL DA RELAÇÃO DE LISBOA. Processo número 1950/17.0 T9LSB-A.L1-5 de 06 de fevereiro de 2018.
[26] TRIBUNAL DA RELAÇÃO DE LISBOA. Processo número 184/12.5TELSB-R.L1-3 de 27 de janeiro de 2021.
[27] TRIBUNAL DA RELAÇÃO DE LISBOA. Processo número 10626/18.0T9LSB-B.L1 de 15 de junho de 2022.

A problemática do despacho prévio do juiz tem também vindo a gerar discussão num outro campo de ação.

De acordo com o artigo 15.º número 3 alínea a) da Lei do Cibercrime, texto relativo à pesquisa de dados informáticos, o órgão de polícia criminal pode proceder à pesquisa sem que haja uma prévia autorização da autoridade judiciária, *in casu*, quando a mesma for voluntariamente consentida por quem tiver a disponibilidade ou o controlo desses mesmos dados.

É realizada uma busca a uma empresa e essa busca é consentida pelos detentores do controlo dos dados, podendo, o próprio Ministério Público autorizar a realização da pesquisa informática. Na diligência, se for encontrado correio eletrónico suspeito, este mesmo correio não pode ser apreendido pelo procurador do Ministério Público, já que é necessária a autorização prévia do juiz.

Este facto está a gerar alguma controvérsia na doutrina e na jurisprudência, porque impede, na prática a concretização destas diligências.

Na perspetiva de Cardoso[28] e de alguma jurisprudência, tal como plasmado num Acórdão do Tribunal da Relação do Porto[29], o artigo 17.º da Lei do Cibercrime não tem aplicabilidade mesmo que exista consentimento por parte daqueles que têm disponibilidade ou controlo dos dados, não sendo necessária a intervenção por despacho prévio do juiz de instrução. Defende-se que este artigo apenas se aplica quando os dados pretendidos não estão acessíveis.

Num recente acórdão do Supremo Tribunal de Justiça[30] refere-se que

> "*na fase de inquérito, compete ao juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente de estas mensagens se encontrarem abertas (lidas) ou fechadas (não lidas), desde que se afigurem ser de grande interesse para descoberta da verdade ou para a prova"*, com os fundamentos do artigo 17.º da Lei do Cibercrime.

Reforçando o citado supra, também nos parece que a lei é perfeitamente clara, ou seja, a diligência carece de uma prévia autorização da autoridade

[28] 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*, *153*, pp. 167-214, 2018.
[29] TRIBUNAL DA RELAÇÃO DO PORTO. Processo número 1145/08.4PBMTS.P1 de 20 de janeiro de 2016.
[30] SUPREMO TRIBUNAL DE JUSTIÇA. Processo número 10/2023 de 10 de novembro de 2023.

judiciária, especificamente do juiz. Este parece-nos ser o verdadeiro espírito da norma, considerando que a lei exige a existência de um despacho judicial prévio para que se possa legitimar a apreensão.

O Tribunal Constitucional[31] chumbou, por unanimidade, o Decreto-Lei aprovado no Parlamento que dava acesso ao Ministério Público, às mensagens de correio eletrónico sem necessidade de autorização prévia de um juiz. Na fundamentação desse acórdão, considera-se que o Ministério Público, uma vez que é o detentor da ação penal, não pode possuir a independência necessária que lhe permita apreciar a necessidade ou a pertinência da apreensão do conteúdo do correio eletrónico. Neste sentido, vai também o parecer 2021/74 da Comissão Nacional de Proteção de Dados[32] e a jurisprudência do Tribunal de Justiça da União Europeia[33].

Este foi também o entendimento do Presidente da República, que, em outubro de 2021, vetou o diploma do parlamento que visava alterar a Lei do Cibercrime, por inconstitucionalidade do artigo 17.º, o qual permitiria a apreensão de correio eletrónico sem ordem prévia de um juiz, por violação do princípio da reserva de juiz e das garantias constitucionais de defesa em processo penal.

4. Considerações finais

Procurou-se, ao longo deste trabalho, contribuir para uma reflexão acerca da conexão entre a Lei do Cibercrime e o Código de Processo Penal, que permita esclarecer possíveis divergências normativas entre os dois diplomas.

No regime da prova em suporte eletrónico, a promulgação da Lei do Cibercrime veio, de facto, superar uma lacuna normativa que existia no ordenamento jurídico-penal em Portugal, no entanto, criou problemas na articulação entre os dois diplomas.

Em nosso entender, a apreensão de correio eletrónico ou de registos de natureza semelhante carecem de despacho prévio do juiz de instrução, o qual deve ser também o primeiro a tomar conhecimento do conteúdo das mensagens.

No nosso entendimento, o despacho do Ministério Público que ordene a apreensão de correio eletrónico tem caráter nulo, assim como também é nula a

[31] TRIBUNAL CONSTITUCIONAL. Processo número 687 de 29 de julho de 2021.
[32] https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2021&type=4&ent=&pgd=2
[33] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Acórdão C-746/18, de 02 de março de 2018.

omissão da análise da correspondência apreendida pelo juiz de instrução. A intervenção do juiz, com a sua necessária imparcialidade e independência, constitui a verdadeira forma de salvaguarda dos direitos constitucionalmente estabelecidos, funcionando como uma competência de cariz exclusivo e não delegável.

Como forma de reflexão final, realça-se a importância da criação de um regime de apreensão de correio eletrónico que seja independente, mas também autossuficiente, no qual estejam bem delimitadas as competências do Ministério Público e do próprio juiz.

REFERÊNCIAS BIBLIOGRÁFICAS

BACELAR GOUVEIA. Jorge. Direito do Ciberespaço e Segurança Cibernética, *Revista Jurídica Portucalense*, *29*, pp. 59-77, 2021.

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*, *153*, pp. 167-214, 2018.

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, 2007.

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

COSTA ANDRADE, Manuel. *Sobre as proibições de prova em processo penal*, Coimbra, Editora Gestlegal, 2ª edição, 2022.

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

DIAS VENÂNCIO, Pedro. *Lei do Cibercrime: anotada e comentada*, Coimbra, Editora D´Ideias, 2023.

DIAS VENÂNCIO, Pedro. *Lições de Direito do Cibercrime, E da tutela penal dos dados pessoais*, Coimbra, Editora D´Ideias, 2022.

FIDALGO, Sónia. A recolha de prova em suporte eletrónico - em particular a apreensão de correio eletrónico, *Revista Julgar*, *38*, pp. 151-160, 2019.

FIGUEIREDO DIAS, Jorge; COSTA ANDRADE, Manuel. Comentário Conimbricense do Código Penal. Parte Especial. Tomo II. 2ª edição, Coimbra, Editora Gestlegal, 2022.

FIGUEIREDO DIAS, Jorge. *Direito Penal. Questões fundamentais. A doutrina geral do crime*. *Parte geral*, *Tomo I*, Coimbra, Coimbra Editora, 2011.

MARQUES DA SILVA, Germano. *Direito Penal Português*. Lisboa, Universidade Católica Editora, 2020.

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

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

RODRIGUES NUNES, Duarte. *Os crimes previstos na lei do cibercrime, Coimbra*, Editora Gestlegal, 2020.

SIMAS-SANTOS; Manuel; LEAL-HENRIQUES, Manuel; SIMAS-SANTOS, João. *Noções de Processo Penal*, 3ª edição, Lisboa, Rei dos Livros, 2020.

TAIPA DE CARVALHO, Américo. *Direito Penal. Parte Geral. Questões fundamentais e teoria geral do crime*. Lisboa, Editora Universidade Católica, 2022.

VERDELHO, Pedro. *A nova lei do Cibercrime*, Tomo LVIII, Braga, Scientia Jurídica, 2009.

JURISPRUDÊNCIA

SUPREMO TRIBUNAL DE JUSTIÇA. Processo número 10/2023 de 10 de novembro de 2023.
TRIBUNAL DA RELAÇÃO DE LISBOA. Processo número 18/19.0YUSTR-N.L1-PICRS de 20 de fevereiro de 2023.
TRIBUNAL DA RELAÇÃO DE LISBOA. Processo número 10626/18.0T9LSB-B.L1 de 15 de junho de 2022.
TRIBUNAL CONSTITUCIONAL. Processo número 687 de 29 de julho de 2021.
TRIBUNAL DA RELAÇÃO DE LISBOA. Processo número 184/12.5TELSB-R.L1-3 de 27 de janeiro de 2021.
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Acórdão C-746/18, de 02 de março de 2018.
TRIBUNAL DA RELAÇÃO DE LISBOA. Processo número 1950/17.0 T9LSB-A.L1-5 de 06 de fevereiro de 2018.
TRIBUNAL DA RELAÇÃO DO PORTO. Processo número 1145/08.4PBMTS.P1 de 20 de janeiro de 2016.

Data de submissão do artigo: 28/12/2023

Data de aprovação do artigo: 21/03/2024

Edição e propriedade:

Universidade Portucalense Cooperativa de Ensino Superior, CRL

Rua Dr. António Bernardino de Almeida, 541 - 4200-072 Porto

Email: upt@upt.pt