UNIVERSIDADE CATÓLICA PORTUGUESA

A Prova Digital em Processo Penal: Apreensão de Correio Eletrónico

(Proposta de alteração do art. 17.º e Acórdão do Tribunal Constitucional n.º 687/2021)

Eunice Horta Rendeiro Martinho Clemente

Mestrado em Direito

Faculdade de Direito | Escola do Porto

Março de 2022

UNIVERSIDADE CATÓLICA PORTUGUESA

A Prova Digital em Processo Penal: Apreensão de Correio Eletrónico

(Proposta de alteração do Art. 17.º e Acórdão do Tribunal Constitucional n.º 687/2021)

Eunice Horta Rendeiro Martinho Clemente

Orientador: Prof.º Doutor Pedro Miguel Fernandes Freitas

Mestrado em Direito

Faculdade de Direito | Escola do Porto

Março de 2022

AGRADECIMENTOS

A primeira palavra de agradecimento será dirigida ao Dr. Pedro Miguel Freitas, por toda a disponibilidade e, acima de tudo, pela orientação de excelência que me presenteou. Um sentimento de eterna gratidão e admiração.

Aos meus pais, pelo amor sem limites, pela paciência e por todo o apoio incondicional.

À minha avó, a quem dedico todo o meu percurso académico.

A todos os meus amigos, em especial ao Francisco e à Mariana, pelo apoio incondicional, companheirismo e paciência. Obrigada por me ajudarem a manter os pés na terra, pela presença constante e relembrarem-me sempre o que é realmente importante.

"Termino este percurso com a plena convicção de que existem pessoas que nos inspiram a seguir o caminho e outras que nos mantêm inteiros enquanto o percorremos."

RESUMO

As novas tecnologias de informação e comunicação levaram a que as sociedades atuais se tornassem em verdadeiras e permanentes sociedades informacionais e comunicacionais, pelo que a tecnologia tomou de assalto todas os aspetos do nosso dia-a-dia.

Contudo, as comunicações eletrónicas, além dos inegáveis benefícios, expõem-nos a novos e diversificados perigos, incitando a criminalidade informática para categorias bastante evoluídas. Reconhecendo-se a natureza instável, dispersa e imaterial características da prova digital, tornou-se imperativo adequar as leis penais aos novos crimes praticados por meios informáticos, levando o legislador a acrescentar à investigação criminal novos meios de obtenção de prova digital adaptados ao ambiente eletrónico digital, de forma a garantir a integridade e força probatória desta prova.

Deste modo, as interceções e apreensões de correio eletrónicos configuram, atualmente, um dos mais importantes meios de obtenção de prova no combate à criminalidade informática, resultando num novo padrão de investigação criminal, pelo que a criminalidade informático-digital, pelas suas características e natureza, não pode ser investigada em termos clássicos.

Neste contexto, esta dissertação versa sobre as questões processuais respeitantes à apreensão de correio eletrónico, procurando, com este estudo, analisar as disposições processuais vigentes no ordenamento jurídico português que regulam a obtenção da prova digital, pondo em questão a conciliação dos regimes dispostos tanto na Lei do Cibercrime, como nas várias disposições processuais consagradas no Código de Processo Penal relativas à obtenção da prova digital. Analisa-se, também, a proposta de alteração do art. 17.º da Lei do Cibercrime, bem como o recente acórdão do Tribunal Constitucional que deu resposta à referida proposta.

Palavras-Chave: Prova Digital, Cibercrime, Lei do Cibercrime, Direitos Fundamentais, Correio Eletrónico.

ABSTRACT

The new information and communication technologies transformed modern societies into real and permanent informational and communicational societies, since technology stormed every aspect of our daily lives.

However, electronic communications, albeit the undeniable benefits, expose us to novel and diverse hazards, inciting evolved categories of cybercrime. Acknowledging the unstable, disperse and immaterial nature of digital evidence it is imperative to adapt criminal laws to the new crimes committed by electronic means, prompting the legislator to add to criminal investigation new ways to obtain digital evidence, adapted to the digital environment, to guarantee the proof's integrity and evidential value.

Consequently, the electronic mail interceptions and apprehensions currently configure one of the most important means to obtain proof when tackling cybercrime, resulting in a new standard of criminal investigation, that cannot be investigated using the traditional methods, due to its characteristics and nature.

In this context, this dissertation consists of the procedural matters regarding electronic mail apprehensions, with the intention to analyse the current procedural provisions in the Portuguese legal system that regulates the obtention of digital evidence, bringing into discussion the conciliation of the regimes established in the Cybercrime Law and in the various procedural provisions enshrined in the Code of Criminal Procedure regarding the acquisition of digital evidence. The proposal to amend art. 17.º of the Cybercrime Law, as well as the recent ruling by the Constitutional Court that responded to the above-mentioned proposal, will also be analysed.

Keywords: Digital Evidence, Cybercrime, Cybercrime Law, Fundamental Rights, Electronic Mail.

SIGLAS E ABREVIATURAS

AR – Assembleia da República

Art. – Artigo

Arts. – Artigos

Ac. – Acórdão

BVerfG – Tribunal Constitucional Federal da Alemanha

CEDH – Convenção Europeia dos Direitos do Homem

Cf. – Conferir

Cfr. – Confrontar

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

EMS – *Enhanced Messaging Service*

ENISA – *European Union Agency For Cybersecurity*

ISP - *Internet Service Providers*

JIC – Juiz de Instrução Criminal

LCC – Lei do Cibercrime

MMS – *Multimedia Messaging Service*

MP – Ministério Público

N.º - Número

OPC – Órgão de Polícia Criminal

p. – Página

pp. – Páginas

PR – Presidente da República

SMS – *Shot Message Service*

STJ – Supremo Tribunal de Justiça

SWGDE – *Scientific Working Group on Digital Evidence*

ss. – Seguintes

TC – Tribunal Constitucional

TRG – Tribunal da Relação de Guimarães

TRL – Tribunal da Relação de Lisboa

ÍNDICE GERAL

INTRODUÇÃO

As novas tecnologias de informação e comunicação envolveram-se de tal forma no nosso quotidiano, que se tornou possível efetuar compras, pesquisas, comunicações, transações bancárias, entre tantas outras, com uma facilidade inacreditável. Foi uma evolução tal que o ser humano, atualmente, não só se considera um ser social, como também um ser tecnológico, de tal modo que, por exemplo, as redes sociais e de telecomunicações quase se consideram meios indispensáveis à vida humana. Neste sentido, compreende-se que é cada vez maior o número de pessoas com acesso aos novos meios de comunicação eletrónica.

Contudo, todas as vantagens também acarretam desvantagens, isto é, a evolução tecnológica e comunicacional foi adotada para a prática de novos crimes, tal como o desenvolvimento tecnológico contribuiu para que os criminosos conseguissem ocultar as suas identidades, bem como provas que levem à sua descoberta. Assim, podemos afirmar que a cibercriminalidade representa uma nova realidade na sociedade globalizada, com grandes impactos tanto no direito penal, como em processo penal.

Hoje em dia, as apreensões de comunicações eletrónicas configuram um dos mais importantes meios de obtenção de prova no combate à criminalidade informática. Contudo, este tipo de criminalidade, pelas suas características e natureza, não pode ser investigado pelos modos tradicionais, sendo necessário adaptar os métodos de investigação às novas características deste tipo de crimes.

Ora, o ordenamento jurídico português não dispunha de quaisquer normas específicas sobre a recolha de prova em suporte eletrónico, ou mesmo qualquer referência ao termo "correio eletrónico", pelo que se recorria às normas gerais do CPP. Deste modo, emergiu a necessidade de atualização normativa.

A reforma do CPP de 2007, através do artigo 189.º, n.º 1, no âmbito da correspondência eletrónica, dispôs que o regime de escutas telefónicas seria correspondentemente aplicável às conversações ou comunicações transmitidas por correio eletrónico. Porém, foi a Lei n.º 109/2009 que veio regular a matéria do cibercrime em Portugal, dispondo, no seu art. 17.º, que a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, reger-se-ia pelo "regime da apreensão de correspondência previsto no Código de Processo Penal".

No ano de 2021, a AR apresentou uma Proposta de Alteração ao atual art. 17.º da LCC, cujo objetivo seria clarificar o modelo de apreensão de correio eletrónico, particularmente, alterar o disposto no referido artigo relativamente à questão da autorização pelo juiz, através de despacho prévio, de apreensão de correio eletrónico e registos de comunicações de natureza semelhante.

Esta Proposta originou inúmeras controvérsias doutrinárias e jurisprudenciais quanto ao regime de recolha de correio eletrónico e de natureza semelhante, com relevo na temática das competências do JIC e do MP, bem como quanto ao monopólio da primeira leitura do teor do correio eletrónico, debatendo-se em torno da análise da incidência da norma prevista no art. 179.º e do art. 252.º, ambos do CPP.

Nesse sentido, a presente dissertação tem por objetivo tratar do tema da prova digital, mais concretamente, a apreensão de correio eletrónico em processo penal, analisando as normas que regulam essa matéria, apresentando as principais problemáticas, nomeadamente no tocante aos poderes do JIC e MP, analisando, a proposta de alteração do art. 17.º da LCC, bem como o recente acórdão do TC relativo à matéria em questão (Ac. n.º 687/2021).

1. Breve contextualização da Prova no Processo Penal Português

1.1. Os princípios reguladores da Prova

O estudo dos princípios reguladores de processo penal é de extrema importância, pelo simples facto de constituírem parâmetros normativos do direito vigente, mas também por motivos pedagógicos, uma vez que permite apreender os valores fundamentais em que assenta o sistema processual penal vigente. Para além disso tem, também, uma grande importância prática na aplicação do direito processual penal. De entre vários princípios reguladores de processo penal, cumpre estudar os princípios relativos à prova.

Em primeiro lugar, um dos mais importantes princípios será o princípio da legalidade da prova, consagrado no art. 125.º do CPP, estabelecendo que são admissíveis as provas que não forem proibidas por lei. Ora, são provas proibidas por lei todas as que são obtidas mediante tortura, coação, ofensa à integridade, abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32.º, n.º 8, CRP). Já no tocante aos métodos proibidos de prova, serão proibidos todos os métodos utilizados de igual forma que as provas proibidas, porém, sem o consentimento do respetivo titular

(art. 126.º, n.º 1 e 3, CPP), com exceção de alguns casos previstos na lei, tais como os art. 177.º e 187.º do CPP.

A não verificação deste princípio resulta na "(...) *nulidade* das provas obtidas através de métodos proibidos, *não podendo as mesmas serem utilizadas*." [1] (art. 32.º, n.º 8, CRP, art. 126.º, n.º 1 e 3 e art. 118.º, n.º 1, CPP), sendo que à sanção "(...) acresce a *proibição de valoração da prova* obtida através de métodos de prova proibidos, dispondo expressamente o artigo 118º, nº 3, do CPP que as disposições sobre nulidades não prejudicam as normas do Código relativas a proibições de prova."[2]

De seguida, em matéria de apreciação da prova, cumpre saber se esta deve ter na sua génese preceitos legais que predeterminem o valor a ser atribuído (princípio da prova legal) ou se deve basear na sua livre valoração pela entidade competente (princípio da livre apreciação da prova). Este último princípio encontra-se consagrado no art. 127.º do CPP, que dispõe que a prova é apreciada segundo as regras da experiência e livre convicção da entidade competente, salvo quando a lei dispuser de outra forma.

Mesmo sendo um princípio com especial relevo na fase de julgamento, uma vez que nesta fase não valem provas que não forem produzidas ou examinadas em audiência (art. 355.º, n.º 1, CPP), este princípio vale, também, para outras entidades, tais como para o JIC e para o MP, pelo que se torna num princípio geral de processo penal com incidência no decurso de todo o processo[3].

Outros dos princípios de extrema importância para a prova em processo penal será o princípio da investigação ou da verdade material. É sabido que o tribunal não está limitado pela prova dos factos aduzida pela acusação e defesa, mas antes tem o poder-dever de investigação oficiosa[4]. Ora, o princípio da investigação ou da "verdade material", consagrado no art. 340.º, n.º 1 do CPP, é o princípio segundo o qual o tribunal investiga os factos sujeitos a julgamento, independentemente dos contributos da defesa e da acusação, constituindo de forma autónoma as bases para a sua decisão[5].

Sendo definido o objeto do processo pela acusação e delimitado o objeto do julgamento, o tribunal deve procurar a reconstituição histórica dos factos de forma a alcançar a verdade material, pelo que, o tribunal pode ordenar oficiosamente toda a produção de prova que entenda necessária para a descoberta da verdade.

---

[1] ANTUNES, 2021, p. 188.
[2] *Idem*.
[3] ANTUNES, 2021, p. 190.
[4] SILVA, 2017, p. 99.
[5] ANTUNES, 2021, p. 185.

Citando Germano Marques da Silva, este poder-dever de procurar a verdade é "(...) justificado pela necessidade de procurar a *verdade material*, pois que ao processo penal não bastaria uma verdade formal, ou seja, a reconstituição hipotética dos factos feita apenas com base na contribuição probatória das partes, mas a verdade histórica, também designada por *verdade material*".[6]

No que toca aos direitos do arguido, a presunção de inocência é identificada como o princípio *in dubio pro reo*, também conhecido por "benefício da dúvida". Significa que a questão da prova será sempre valorada a favor do arguido, isto é, o arguido tem sempre o direito a ser absolvido ou a ser declarado inocente, caso não seja feita a prova absoluta da sua culpabilidade[7]. Em bom rigor, é meramente um princípio lógico de prova, pois se o tribunal não lograr a prova dos factos que constituem o objeto do processo, deve considerar a acusação não provada e, consequentemente, não aplicar qualquer sanção ao arguido, uma vez que a acusação é considerada infundada.

Este princípio encontra fundamento jurídico-constitucional no art. 32.º, n.º 2 da CRP, ao declarar que todo o arguido presume-se inocente até trânsito em julgado da sentença[8]. Produzida a prova, segundo o disposto nos art. 340.º e 341.º do CPP, o tribunal aprecia a mesma, ao abrigo das regras da experiência e da sua livre convicção, que deve ser sempre objetivável e motivável (art. 127.º, CPP). Desta forma, conclui de três formas: ou que foi produzida prova dos factos imputados ao arguido, resultando em que os dados foram dados como provados; caso contrário, que não foi produzida prova de tais factos, pelo que os dados não são dados como provados; ou, ainda, apesar da prova produzida, ficou aquém da dúvida razoável, pelo que se dá, também, os factos como provados.

Não menos importante, cumpre referir o princípio da não taxatividade[9], uma vez que o CPP consagra a regra da não taxatividade dos meios de prova. Contrariamente ao art. 189.º do CPP italiano[10], a lei portuguesa não estabelece um critério substantivo especial para a admissibilidade das provas não previstas na lei, pelo que a admissibilidade das provas não previstas na lei rege-se pelos critérios substantivos gerais do art. 340.º. Os meios de obtenção de prova também se encontram subordinados a este princípio da não

[6] SILVA, 2017, p. 100.
[7] SILVA, 2017, p. 96.
[8] ANTUNES, 2021, p. 193.
[9] ALBUQUERQUE, 2011.
[10] O art. 189.º, n.º 1, do CPP italiano afirma "*Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova*.".

taxatividade. Porém, quando o meio de obtenção de prova acarretar um alto grau de intrusão na privacidade do suspeito, ele deve ser previsto por uma lei expressa.

Resta considerar que a obtenção da prova digital deve seguir determinados princípios reguladores autónomos[11], que se cumulam com os princípios referentes à prova no processo penal, suprarreferidos, pelo que a prova digital deve ver reconhecidos os princípios específicos respeitantes às características da prova concreta, para além dos princípios genéricos, como será analisado no ponto seguinte.

1.2. Particularmente: a Cadeia de Custódia da Prova e os princípios da Prova Digital

O instituto da prova e respetiva cadeia de custódia tem uma relação umbilical com os princípios constitucionais de processo penal, tal como afirma Miguel Reale "juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados num sistema de conceitos relativos a dada proporção de realidade".[12]

A verdade processual penal não tem valor absoluto, não podendo ser alcançada a qualquer preço, pelo que é necessário respeitar sempre a dignidade da pessoa humana, bem como os direitos fundamentais, prevendo o CPP regras expressas.

De entre vários princípios, destaca-se o princípio do devido processo legal dotado de todas as garantias processuais, estando a efetividade deste princípio diretamente ligada à vigência de princípios constitucionais de processo penal, como é o caso dos princípios da legalidade e da constitucionalidade da atuação dos operadores judiciários, o principio da jurisdicionalidade de todo o processo, o princípio da prossecução do interesse público e da prossecução dos direitos e interesses particulares, o principio da boa fé e da confiança e, por fim, o principio da lealdade (transparência) da atividade dos autores judiciários. "Estes princípios dão a roupagem e a força vinculativa à ação dos operadores judiciários para que se garanta uma efetividade do princípio do devido processo legal com todas as garantias de defesa."[13]. Observa-se a opinião de Claus Roxin quando afirma que o processo penal está abeberado de hierarquias éticas e jurídicas do Estado, de que não é possível abdicar na procura por um valor não absoluto que é a verdade.[14]

---

[11] *International Hi-Tech Crime and Forensics Conference*, https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/ , acedido a 04/05/2022.

[12] REALE, 2010, p. 60.

[13] VALENTE, 2021, p. 47.

[14] ROXIN, Claus, *Derecho Procesal Penal*, 2000, p. 191 *cit. por* VALENTE, 2021, p. 47.

Outros dois princípios igualmente importantes são os princípios da identidade e autenticidade na e da cadeia de custódia da prova. A cadeia de custódia da prova é considerada uma técnica jurídico-processual que garante a identidade e a autenticidade da prova de todo o processo penal, pelo que todo o procedimento está obrigado a respeitar e promover os princípios constitucionais de processo penal diretamente ligados ao instituto da prova, cuja violação vicia a sua utilização no processo. Assim, caso haja uma ausência de controlo jurisdicional ou controlo efetivo na tutela e garantia destes dois princípios em análise, resulta em proibições de produção de prova, ou seja, na inadmissibilidade da prova e, caso seja submetida a julgamento, na inadmissibilidade de valoração da prova.

Deste modo, é de concluir que a verdade não pode ser alcançada a todo o custo, impondo-se que os autores judiciários (MP, juiz, polícia criminal, peritos, advogados, entre outros) atuem dentro do quadro da legalidade material válida em cada momento e espaço do processo penal[15].

Fala-se de outro princípio igualmente relevante, o princípio da indisponibilidade das competências. De uma forma mais concreta, é de extrema importância que os autores judiciários e processuais ligados ao processo de aquisição, coleta e conservação da prova façam um juízo de constitucionalidade que, desde logo, impõe um juízo de competência constitucional da atuação do órgão de polícia criminal ou de polícia judiciária. É possível afirmar-se que não é da competência dos elementos da polícia criminal a função de perito criminal.

O princípio da indisponibilidade da competência para apurar, adquirir, recolher e conservar a prova (custódia), para futuro exame pericial, deve verificar-se no quadro do procedimento da cadeia de custódia da prova. Ou seja, a violação do lacre só é admissível por perito criminal, não sendo submissível às funções da autoridade de polícia criminal ou de qualquer outro órgão com funções de polícia judiciária, incluindo o delegado de polícia[16]. Caso contrário, resulta numa violação deste princípio em apreço, sendo este considerado um dos maiores limites ao poder de perseguir criminalmente alguém, bem como ao poder de dirigir e controlar a atividade de investigação.

Nos termos do art. 151.º do CPP, o recurso à prova pericial está submisso ao trabalho de um perito, tendo lugar quando a perceção ou apreciação dos factos exigem especiais conhecimentos técnicos, científicos ou artísticos. Por outro lado, à polícia

[15] VALENTE, 2021, p. 49.
[16] *Idem,* p. 52.

criminal cabe proceder à descoberta, apreensão e conservação da prova (cf. art. 249.º, n. º1, CPP e art. 272.º, n.º 2 e 3, em conjugação com o art. 202.º, n.º 3 da CRP).

Ademais, o elemento policial não pode aceder à coisa que se encontra sob cadeia de custódia da prova, pelo que, tendo em conta o sentido dos art. 252.º e 179.º do CPP, cabe-lhe garantir e tutelar a impenetrabilidade das provas apreendidas até à intervenção dos peritos, para que não se criem dúvidas ou suspeitas sobre a identidade (originalidade) e a autenticidade (integralidade) da prova apreendida.

Neste sentido, leva-nos a destacar outro princípio – o princípio do interesse público na realização da justiça – uma vez que, apesar da realização da justiça deva ser efetiva, é de realçar que essa mesma realização deve observar limites, tais como a intocabilidade da integridade da prova, bem como a legalidade material e formal dos métodos de obtenção da prova e das técnicas de conservação e manutenção, sem quaisquer suspeitas de manipulação ou alteração do conteúdo da prova. Resumidamente, a prova tem que parecer e ser honesta, imaculada.

A prossecução do interesse público na realização da justiça tem valores que não podem ser afastados, como é o caso da atividade dos autores judiciários ter de respeitar a legalidade material e processual, respeitar a confiança entre todos os cidadãos, obedecer a uma ética republicada democrática que nega a justiça a todo o custo, devendo ter em conta que este princípio em debate não é absoluto, pois tem como limite o princípio do respeito dos direitos e interesses legítimos dos particulares (direito a um devido processo legal submetido ao princípio da ampla defesa e do contraditório, conforme os art. 20.º, n.º 4 e 32.º, n.º 1 e 5, CRP).

Nesta sequência, desenvolvem um caráter de relevância o princípio da boa-fé e confiança, tendo em conta que aos autores judiciários é imposta uma atuação de confiança, de modo que a cadeia de custódia da prova seja respeitada e a prova possa ser submetida à produção e valoração em sede de audiência de discussão e julgamento.

O princípio da boa-fé apresenta-se como "instrumento garantístico das expectativas e da confiança dos particulares, geradas a partir de comportamentos"[17] dos órgãos do Estado, neste caso, da polícia criminal. Tal como defende Manuel Guedes Valente, "o princípio da boa-fé não é, hoje, um mero princípio de intenção moral, mas um verdadeiro princípio legitimador da atividade da administração da justiça por parte do Estado, sendo de grande relevância muito em especial para a atuação da polícia

[17] PINHEIRO e FERNANDES, 1999, p. 547.

criminal."[18]. Desta forma, o instituto da prova e respetiva cadeia de custódia, exige à autoridade policial uma atuação com base no respeito integral pelo princípio da boa-fé, que se densifica no núcleo do princípio da lealdade.

Analisando este referido princípio da lealdade e citando Claus Roxin, será "o mais alto princípio de todo o processo penal: o de exigência de *fair trial*, de um procedimento leal"[19]. Um Estado de direito democrático que se baseia no respeito pela dignidade da pessoa humana e na vontade popular exige aos operadores judiciários que, acima de tudo, promovam, através das suas atuações, o respeito e a garantia dos direitos fundamentais da pessoa, de forma a alcançar a paz jurídica e social e unifiquem a defesa da legalidade democrática. Nas palavras de Germano Marques da Silva, este princípio deve traduzir "uma maneira de ser da investigação e obtenção das provas em conformidade com o respeito dos direitos da pessoa e a dignidade da justiça"[20]. Assim, este princípio será integrante do processo penal, uma vez que impõe aos autores judiciários a obrigatoriedade de atuação observando o respeito pelos valores da pessoa humana, tais como a sua dignidade, integridade pessoal, a sua liberdade de formação e manifestação da sua vontade perante a sociedade. Este princípio não se encontra plasmado nas Constituições, porém afere-se do art. 32.º, n.º 8 da CRP ao proibir a admissibilidade de provas ilícitas em processo penal.

Por último, mas não menos importante, é de referir o princípio da jurisdicionalidade (art. 20.º, n.º 4, CRP e art. 6.º da CEDH) que impõe que certos atos e diligências processuais sejam precedidos de ordem ou determinação judicial, isto é, exige uma tutela reforçada por meio do princípio da jurisdicionalidade. Esta tutela não se esgota na determinação ou ordem prévia judicial, uma vez que impõe uma série de fundamentação da necessidade, imprescindibilidade e indispensabilidade de recurso a este tipo de meios assentes na intimidade e na vida privada e familiar, por parte da polícia criminal, do MP e do juiz que determina ou ordena esse ato ou diligência processual.

Em Portugal, o acesso a dados informáticos ou dados de tráfego incluídos em sistemas informativos, carece de prévia autorização judiciária, devendo esta presidir à diligência de pesquisa e apreensão dos dados informáticos, ao abrigo do art. 15.º, n.º 1, conjugado com o art. 16.º, n.º 1 e 3, ambos da LCC. Só serão exceção a esta regra as

[18] VALENTE, 2021, p. 60.

[19] ROXIN, Claus, *Derecho Procesal Penal*, 2000, p. 13, 101 e 108, *cit. por* VALENTE, 2021, p. 61

[20] SILVA, 2010, p. 53 e 161.

situações de elevada perigosidade, como é o caso de terrorismo, crime violento ou organizado caso haja indícios da prática iminente de crime que coloque em risco a vida ou integridade de qualquer pessoa, porém, com comunicação imediata à autoridade judiciária competente para a apreciação e validação[21]. À polícia criminal não compete o acesso a este tipo de conteúdo privado, sob pena de nulidade da diligência e das provas meio obtidas, bem como da prova resultado, sendo esta nulidade de natureza insanável, pelo que torna inexistente o ato e recolha da prova, sendo inadmissível como prova do processo.

Assim, podemos concluir que esta atividade de obtenção e produção de prova tem que observar o respeito pelos referidos direitos fundamentais, bem como pelas garantias consagradas na CRP e na lei em geral. No entanto, a prova digital também é alvo de princípios mais particulares. A este propósito, Benjamim Silva Rodrigues oferece um elenco de princípios a observar, resultando na criação de um novo padrão de investigação em processo penal[22].

Além da aplicação dos princípios específicos que se prendem com a prova digital, aplicam-se, também, os princípios vigentes em matéria processual penal, em geral, e em matéria da prova em processo penal, em particular. Está, então, em causa o princípio da cumulação dos princípios processuais penais em matéria probatória, juntamente com os princípios particulares à prova digital, não sendo legítimo a omissão dos primeiros por estes últimos, ou a preferência destes últimos em detrimento dos primeiros.

De seguida e de forma a garantir a integridade da prova obtida durante o processo de recolha, armazenamento e tratamento, a prova digital deverá respeitar um princípio de não alteração da prova no ato de recolha, ou seja, é exigido que, durante o processo de investigação, o investigador não observe qualquer conduta que contamine os dados obtidos com elementos alheios ao sistema ou rede informáticos investigados[23]. Com este princípio, é aconselhado um especial esforço dos órgãos formais de controlo no sentido de garantir que, mesmo não sendo com má-fé, se não introduzam alterações ou contaminem os dados com elementos estranhos ao sistema ou rede informáticos, retirando por completo a força probatória das provas recolhidas, anulando qualquer valor para o processo.

[21] VALENTE, 2021, p. 67.
[22] RODRIGUES, 2011, p. 41 e ss.
[23] RODRIGUES, 2009, p. 726.

Neste âmbito, é igualmente relevante o princípio da especialização ou qualificação do pessoal adstrito à investigação forense digital, uma vez que as fases de acesso, recolha, conservação e análise competem a entidades especializadas no núcleo dos órgãos formais de controlo que, dotadas de conhecimentos técnico-científicos adequados, impedem o corrompimento ou o mau manuseamento da prova e subsequente inadmissibilidade desta no processo penal. Afirma Eoghan Casey que "A documentação é uma parte crítica de cada etapa"[24] e, também, "O controlo eficaz do caso também exige que os examinadores documentem suas ações, não apenas no início, mas também durante todo o processo da descoberta digital"[25].

A integridade da prova refere-se à preservação desta numa forma completa, sem quaisquer alterações intencionais ou não intencionais, ou seja, refere-se à preservação da evidência na sua forma original. Porém, embora a integridade da prova seja um ideal na análise digital, muitas vezes não é possível de se alcançar, uma vez que os dados se modificam, inevitavelmente, em redes e sistemas de computador ativos durante as investigações. Por isso mesmo, a documentação de todas as etapas da investigação é um objetivo importante[26]. Assim, no seguimento desta ideia, outro princípio consiste na garantia de documentação em todas as fases processuais (acesso, recolha, armazenamento, transferência, preservação e apresentação ou repetição da prova digital).

A documentação de todas as fases de obtenção e valoração (no fundo, de tratamento) da prova digital pretende exprimir a ideia de que se afigura indispensável, uma vez que é o que permite a realização de uma "cadeia de controlo"[27], ou seja, de garantia de validade da prova digital. Por um lado, porque a repetição da prova pode, por vezes, só ser exequível se for possível a análise da documentação das fases que conduziram à sua produção. Por outro lado, a observância deste princípio conduz a um controlo rigoroso da atividade dos órgãos responsáveis pela obtenção da prova digital.

Ademais, segundo o princípio de responsabilidade pessoal, cada profissional que intervenha na investigação digital terá a responsabilidade de controlar pessoalmente a cadeia de custódia das provas que ele recolher ou produzir, de forma a garantir a força probatória das mesmas, sob pena de uma vez mais, se perturbar a força probatória daquela evidência em particular. Com isto, ficam excluídos do acesso a objetos sob investigação

[24] CASEY, 2010, p. 25.
[25] *Idem*, p. 76.
[26] ARNES, p. 6.
[27] Noção adotada pelo SWGDE, https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm, acedido a 04/03/2022.

qualquer terceiro alheio à investigação, pois a tendência é para a pessoalidade no tratamento da prova digital, isto é, do profissional que legitimamente recolhe, manuseia, analisa, apresenta e explica a prova ao processo em que ela se obtém e valora.

O caráter importantíssimo dado à prova digital resulta em que cada prova recolhida, manuseada, analisada e fundamentada seja feita apenas por um perito ou conjunto de peritos tecnicamente qualificados e identificados no processo.

Por fim, o último princípio que deverá regular a prova digital consiste numa responsabilização repartida dos vários intervenientes na produção da prova no respeito dos princípios orientadores em matéria de obtenção e valoração da prova. Por outras palavras, cabe a cada órgão ou perito encarregue pela recolha e armazenamento da prova digital, o dever de ser inteiramente responsável pelo material que se encontra sob a investigação e custódia dele, ou seja, cada interveniente na produção ou obtenção de dada prova tem que se assegurar pessoalmente do cumprimento dos princípios de produção, análise e descrição da prova digital para, assim, em conjunto e de maneira complementar com os restantes órgãos ou peritos, contribuir para a preservação e manutenção da integridade, fiabilidade e valor probatório da prova obtida em ambiente digital.

Todavia, a Agência da União Europeia para a cibersegurança (ENISA) divulgou cinco princípios fundamentais relativos à obtenção e recolha de prova digital: o princípio da integridade dos dados (esta integridade dos dados deve ser preservada, garantindo que os dados não sejam manipulados); o princípio da cadeia de custódia da prova (adotar uma cadeia de custódia de forma a garantir a autenticidade e integridade da prova); o princípio do apoio especializado (apoio que deve ser requerido sempre que o âmbito da prova ultrapasse os conhecimentos dos investigadores); o princípio da formação profissional (uma formação contínua e adequada de forma a garantir uma apreensão de prova íntegra e eficaz); e, por último, o princípio da legalidade (garantir o respeito por todos os princípios suprarreferidos, bem como o cumprimento da lei)[28].

Para concluir, de forma a garantir a validade da prova digital ao longo do processo de investigação, as fases processuais da prova deverão ser regidas por regras de cumprimento imperativo, sendo relevante, por exemplo, a documentação de qualquer operação efetuada, tal como foi suprarreferido, bem como a intervenção no processo das entidades tecnicamente aptas para que seja garantida a validade da prova.

---

[28] https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders> , acedido a 04/03/2022.

2. A Prova Digital

2.1. Conceito e Características

Inserido no Livro III do CPP (Da Prova), entende-se que a prova é um dos instrumentos fundamentais para a descoberta da verdade quando estamos perante um crime. O art. 125.º do CPP consagra o princípio da admissibilidade de todas as provas que não sejam proibidas por lei, pelo que, todas as provas de caráter digital são admitidas, desde que a sua obtenção tenha sido feita dentro dos critérios da legalidade e objetividade.

Contudo, não existe uma aceção concreta para a figura da prova digital, no entanto, destacam-se alguns autores que expõem uma definição deste conceito. Começando por Benjamim Silva Rodrigues, define a prova digital como "qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital"[29]. Por outro lado, segundo a opinião de Armando Dias Ramos, a prova digital define-se como a "informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"[30].

Face ao exposto, de forma a assegurar a força probatória da prova digital, bem como a sua validade, é imprescindível estudar as características e princípios que a regulam. É de fácil perceção de que a prova digital necessita de ser tratada de uma forma mais delicada, uma vez que ao mínimo descuido pode torná-la inutilizável. Tal como refere Armando Dias Ramos, "(...) a apreensão da prova digital não requer o mesmo tratamento que é dado quando se apreende uma carta ou um outro qualquer documento, por exemplo."[31]

No seguimento desta ideia, em 1999 realizou-se uma conferência em Londres (*International Hi-tech Crime and Forensic Conference*), onde foram apresentadas, pelo SWGDE, algumas definições, *standards* e princípios pertinentes, de forma a expressar à comunidade forense internacional a natureza e a força probatória da figura da prova digital. O propósito desta conferência teve que ver com o crescimento da era digital, marcado pelo aparecimento de uma quantidade colossal de dispositivos eletrónicos para

[29] RODRIGUES, 2009, p. 722.
[30] RAMOS, 2014, p. 86.
[31] *Idem*, p. 88.

além do computador. "Do ponto de vista da aplicação da lei, mais informações que servem como moeda no processo judicial estão a ser armazenadas, transmitidas ou processadas em formato digital."[32]. Esta situação levou a que todas as nações tivessem a capacidade de apreender e preservar as provas digitais para a sua própria defesa, pelo que o SWGDE tentou definir estes *standards* e princípios sobre a prova digital.

Deste modo, em primeiro lugar, a prova digital terá que estar em conformidade com o sistema legal probatório vigorante no processo penal português e, de forma a este tipo de prova ser admitida noutros países, deverá estar, também, em conformidade com o modelo vigente internacionalmente em matéria de prova digital.

Ademais, estando inserida num meio complexo e de apreensão complicada, este tipo de prova deve apresentar-se numa linguagem simples, clara e precisa, observando os termos fundamentais para a investigação. Não obstante, deve ser uma prova durável, sendo que as entidades competentes devem tomar medidas de maneira a garantir a sua conservação.

Por fim e de modo a garantir a sua integridade e força probatória, a prova digital deverá ser produzida observando todos os critérios essenciais, mantendo o rigor e inspirando segurança ao agente que dela fizer uso, pelo que, para tal, é primordial que se verifique conformidade na produção de prova, devendo existir correspondência na sequência dos princípios fundamentais da prova digital em todas as fases do processo.

2.2. As dificuldades colocadas pela Prova Digital

A prova digital integra várias condições que a tornam distinta, vulnerável e especial e, tal como observa Rita Santos[33], as técnicas de recolha e produção da prova digital são diferentes das utilizadas na obtenção dos habituais meios de obtenção de prova, pelo que as primeiras não se satisfazem com as técnicas habituais. A quantidade gigantesca de informação digital que pode ser criada, modificada ou eliminada, em qualquer parte do mundo, juntamente com o incessante avanço dos sistemas de informação, impõe que a investigação se aperfeiçoe e se muna de instrumentos específicos de forma a garantir a integridade deste tipo de prova em questão. Assim,

[32] Retirado do site online do FBI: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm, acedido a 04/03/2022.

[33] SANTOS, 2005, p. 24.

deduz-se que a prova digital deve ser recolhida o mais célere possível, observando todos os cuidados exigidos, sob pena de perder a sua integridade.

O caráter temporário é analisado pela forma como a prova digital pode deixar de existir com o decurso do tempo, e mesmo já existindo legislação que imponha aos provedores de serviços de *Internet* (ISP's) que façam a ressalva dos dados de tráfego[34], este caráter temporário continua a existir, pois basta que a prova não seja produzida, ou seja, que não seja possível de chegar à mesma, ou que não seja salvaguardada no espaço de um ano (período a que os ISP's estão obrigados a guardar os dados relativos às comunicações) para que toda a investigação seja um falhanço e não se identifiquem os criminosos. Para além de temporária, a prova digital é frágil e modificável, resultando numa necessidade acrescida de cuidados a ter.

É uma prova fungível porque os dados informáticos facilmente podem ser substituídos por outros, pelo que, antes da sua recolha, deve ser rigorosamente identificada, não correndo o risco de ser alterada ou de desaparecer, garantindo, assim, a sua força probatória. Porém, existindo essas possibilidades de alteração ou desaparecimento, este tipo de prova é considerado volátil e instável, tornando-se ainda mais complicada a sua apreensão. É de grande volatilidade uma vez que podem ser omitidas ou excluídas do suporte original, resultando uma maior dificuldade em encontrá-las, sendo necessário o uso de ferramentas específicas para tal.

Não menos importante, este tipo de prova consiste numa prova imaterial, logo, impõe ao investigador conhecimentos técnicos e científicos específicos, sendo que esta necessidade deve-se, particularmente, à complexidade da prova digital.

Igualmente importante será mencionar o transporte de material que tenha sido apreendido no âmbito das "buscas digitais". Sendo considerado de enorme fragilidade, deve ser, por exemplo, afastado de campos eletromagnéticos tais como altifalantes, janelas ou bancos aquecidos, e deve ser transportado em sacos anti estáticos.

Quando não for passível de serem cumpridos todos os procedimentos necessários para prova digital ter força probatória, poderá resultar no facto de não se conseguir realizar uma perícia justa, por outras palavras, não será possível reunir elementos de prova

[34] De acordo com o art. 2º, alínea c), da Lei 109/2009, dados de tráfico definem-se como "*os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente".*

que, no âmbito de audiência e julgamento, possam ser valorados justamente e relevantes para a discussão da causa.

As características excecionais da prova digital, mais concretamente o facto de ser temporal, frágil, dispersa, volátil, alterável e imaterial, tornam a prova digital numa prova complexa e carecida de uma especial interpretação, pelo que "as ações de investigação criminal relativas à prova digital exigem aprofundados conhecimentos informáticos e, muitas vezes, meios técnicos e tecnológicos de ponta."[35]. Hoje em dia torna-se indispensável falar-se da ciência forense digital, não só como meio de investigação, mas especialmente para que se determinem procedimentos, princípios e regras que sustentem a integridade, fiabilidade e inalterabilidade deste tipo de prova.

2.3. A Lei n.º 109/2009, de 15 de setembro

Atualmente, sabe-se que as comunicações realizadas através da *Internet* resultaram em mudanças profundas na forma como comunicamos, porém, também nos expuseram a novos riscos, pelo que, a par desta evolução, seria imperativo adaptar as leis penais à atual sociedade da informação, sendo criados novos tipos legais de crimes, preenchendo-se lacunas legais no nosso ordenamento jurídico.

A prova digital carece de uma intervenção legislativa racional, o que não se verifica na realidade, visto que a atual situação legislativa manifesta inconsistências. Deste modo, a primeira lei que veio regular a matéria de cibercrime em Portugal foi a Lei n.º 109/91, de 17 de agosto, a lei da criminalidade informática, que terá sido expressamente revogada por ter se tornado desatualizada. A lei terá sido revogada, uma vez que apenas tratava do direito substantivo relativo aos crimes informáticos, sendo que as normas do CP seriam subsidiárias em relação aos crimes nela previstos, conforme dispunha o art. 1.º da antiga lei. No tocante à matéria processual de cibercrime, esta era regulada pelo artigo 189.º do CPP, sendo que este código sofreu uma reforma em 2007 através da Lei n.º 48/2007, de 29 de agosto, de forma a abranger a recolha de prova eletrónica, na medida em que o disposto nos art. 187.º e 188.º, relacionados com as escutas telefónicas, "é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio

[35] MILITÃO, p. 261.

eletrónico ou outras formas de transmissão de dados por via telemática (...)"[36]. Entretanto, com o passar do tempo e, consequentemente, com a evolução informática, a Lei n.º 109/91 desatualizou-se, pois foram emergindo novos crimes informáticos que não eram regulados pela lei portuguesa, porém já seriam regulados por legislações europeias e instrumentos internacionais.

Em Portugal, através da Resolução n.º 88/2009 da AR e Decreto n.º 92/2009 do PR, ambos publicados a 15 de setembro, Portugal ratificou a Convenção sobre o Cibercrime, adotada em Budapeste em 23 de novembro de 2001, sendo assim, aprovada a atual Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro.

Com a evolução dos crimes informáticos, os danos por eles causados podem fazer-se sentir em múltiplas jurisdições, pelo que se deve encarar este tipo de crimes à escala mundial, daí que, com esta Convenção, seja expressa a necessidade dos vários Estados se dotarem de instrumentos processuais que ajudem a comprovar os crimes digitais, uma vez que a cooperação internacional facilita e ajuda na recolha de prova. Assim, esta Convenção foi criada com o intuito de harmonizar legislações e os crimes nelas previstos, bem como estender às jurisdições dos Estados signatários determinados instrumentos processuais de prova adequados à investigação de crimes informáticos e, não menos importante, pretendeu facilitar a cooperação internacional e viabilizar investigações.

A LCC transpôs para a ordem jurídica portuguesa a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistema de informação, adaptando, assim, o direito interno à Convenção sobre o Cibercrime. Desta transposição para a ordem jurídica interna, a Lei n.º 109/2009 veio consagrar, nos termos do seu art. 1.º, n.º 1, "disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico (...)".

No âmbito da LCC, Pedro Venâncio defende que o catálogo de medidas processuais deve ser observado de forma integrada, "analisado como um todo, pois em muitos aspetos práticos se relacionam e complementam"[37], visto que o objetivo será o mesmo, ou seja, de aceder a dados informáticos essenciais à investigação.

Não obstante, seguindo a opinião de Germano Marques Da Silva, conclui-se que a ordem pública sofre maior perturbação com a violação de direitos fundamentais do que "(...) pela não repressão de alguns crimes, por mais graves que sejam, pois são sempre

[36] Art. 189º, nº1, CPP.
[37] VENÂNCIO, 2011, p. 99.

muitos, porventura maioria, os que não são punidos, por não descobertos, sejam quais forem os métodos de investigação utilizados"[38].

Ora, tendo em conta a Exposição de Motivos da Proposta de Lei n.º 289/X/4ª, que serviu de base ao texto da LCC, ao invés de se concretizar uma alteração das várias fontes normativas relativas à criminalidade informática, optou-se por englobar num só diploma legal todas as disposições relativas ao sector da cibercriminalidade, por ser a solução que se mais se coaduna com a tradição portuguesa[39].

Perante isto, o legislador português, tal como o legislador alemão, incluiu num único diploma legal todo o conjunto de disposições relativas aos crimes informáticos. Porém, como refere Manuel da Costa Andrade, o legislador alemão tem vindo ao longo do tempo a "erigir um regime unificado e sistematizado dos meios ocultos de investigação e assegurar o respeito, neste domínio, da área nuclear inviolável da intimidade."[40], pelo que os meios ocultos de investigação passam a não estarem regulados em leis extravagantes. Seguindo esta linha de pensamento, João Conde Correia, em vez de "(...) optar por poucas leis, simples e claras o legislador escolheu a via incerta da pluralidade e da complexidade, gerando um sistema anárquico, onde, muitas vezes, nem a letra, nem o seu espírito, nem, tão pouco, a sua história fornecem a bússola necessária para encontrar o caminho mais seguro."[41].

Posto isto, é de notar que esta nova LCC se caracteriza como inovadora, uma vez que, para além de ter previsto crimes informáticos que antes não eram regulados, incluiu novos termos, tais como "dados informáticos", "dados de tráfego" e "fornecedor de serviços". Além do mais, foi o primeiro diploma legal a contemplar na ordem jurídica portuguesa, um regime específico de obtenção da prova digital, incluindo um conjunto de novos e diferentes meios de obtenção de prova, de entre eles a preservação expedita de dados (art. 12.º, LCC), a revelação expedita de dados de tráfego (art. 13.º, LCC) e a injunção para apresentação ou concessão do acesso a dados (art. 14.º, LCC).

Como referido no Ac. do TRL, de 22 de Janeiro de 2013, a Lei n.º 109/2009, ao prever um regime jurídico específico, conseguiu superar a lacuna da antiga lei da

[38] ALVES; GONÇALVES, 2009, p. 71.

[39] Exposição dos Motivos da Proposta de Lei nº. 289/X/4ª, https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c637939595447566e4c305276593356745a57353062334e4a626d6c6a6157463061585a684c7a45324f544a684e7a63344c57457a4f4751744e474934595330344d5459304c544d345a4459315a6a59784e444d304f53356b62324d3d&fich=1692a778-a38d-4b8a-8164-38d65f614349.doc&Inline=true, acedido a 04/03/2022.

[40] ANDRADE, 2009, p. 24.

[41] CORREIA, 2018, p. 23.

criminalidade informática que "(...) por não conter essas normas processuais que adequassem o regime legal às particularidades da investigação "empurrou" a jurisprudência para a interpretação de que só em relação a crimes de catálogo seria possível a obtenção de certo tipo de dados como os dados de tráfego e mercê da intervenção do juiz de instrução." [42].

Além do mais, tal como é referido na Exposição de Motivos, era urgente ultrapassar o regime de 2009, de modo a fornecer ao sistema processual normas que possibilitassem a obtenção de dados de tráfego, bem como a realização de interceções de comunicações em investigações de crimes praticados no ambiente virtual, pelo que esta nova lei serviu como uma forma de corrigir uma lacuna que existia no sistema processual penal português.

Ademais, esta lei do cibercrime veio adotar um regime processual não só aplicável a processos relativos a crimes previstos na respetiva lei, como também a processos relativos a crimes cometidos através de um sistema informático ou em qualquer processo criminal em que seja útil proceder à recolha de provas digitais, ao abrigo do seu art. 11.º.

Importa, também, ter em conta que todas as medidas, sejam gerais ou excecionais, bem como as obrigações previstas na LCC, cumulam-se com as que se encontram estabelecidas no CPP, em tudo o que as não contrarie.

Para concluir, denota-se que a LCC, bem como os diplomas conexos, "tiveram em vista responder aos apelos dos que reivindicavam a densificação, facilitação, agilização, enfim, o eficientismo dessas medidas."[43]

Deste modo, tanto se exige uma maior ponderação dos valores em sede de interpretação e aplicação por parte das autoridades competentes, respeitando o princípio da proibição do excesso, como também se exige bastante cuidado, por parte do julgador, na apreciação das provas digitais, tendo em conta a delicadeza das mesmas.

3. Os meios de obtenção da Prova Digital: a apreensão de correio eletrónico

[42] http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument, acedido a 04/03/2022.

[43] MILITÃO, p. 281.

Cada vez mais se torna imprescindível a utilização de mensagens de correio eletrónico e de natureza semelhante que são apreendidas em sistemas informáticos como meio de prova no processo penal, em virtude da grande evolução eletrónica que se tem vivenciado. Desta forma, a lei portuguesa assume que as mensagens de correio eletrónico podem ser usadas como meio de prova, entre outras comunicações, reconhecendo a sua importância como fontes de material probatório.

É, assim, importante analisar o regime jurídico de apreensão de correspondência previsto nos arts. 179.º e 252.º do CPP, de forma a ser possível apreciar a sua compatibilidade com o regime de apreensão de correio eletrónico previsto no art. 17.º da LCC.

O regime previsto neste art. 17.º da LCC tem gerado dificuldades de compatibilização com o disposto no CPP e tem dado lugar a interpretações doutrinais e jurisprudenciais diversas, sobretudo quando a apreensão se faz na fase de inquérito.

Nos termos do art. 179.º, n.º 1, do CPP, o juiz só pode autorizar ou ordenar a apreensão de correspondência quando estiver em causa um crime punível com pena de prisão superior, no seu máximo, a 3 anos (alínea b)). Nos termos do n.º 3 da mesma norma, o juiz que tiver autorizado ou ordenado a apreensão é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se o juiz considerar que a correspondência apreendida é relevante para a prova, fá-la juntar ao processo, caso contrário, restitui-a ao seu titular, não podendo ela ser usada como meio de prova.

Já nos termos do art. 17.º da LCC, à apreensão de correio eletrónico e registos de comunicações de natureza semelhante aplica-se "correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal".

3.1. Código de Processo Penal, os artigos 179.º e 252.º

O regime de apreensão de correspondência previsto no CPP aplica-se à correspondência que se encontra em trânsito entre o remetente e o destinatário, pelo que se assemelha à interceção em tempo real.

A inviolabilidade jurídico-constitucional da correspondência tem como objetivo proteger os bens jurídico-fundamentais da pessoa e, por isso mesmo, a apreensão de correspondência trata-se da "primeira forma especial de apreensão incluída no CPP"[44].

[44] CORREIA, 2019, p. 639.

Na verdade, o legislador limitou-se a criar algumas especificidades que tornam a apreensão de correspondência mais rigorosa e menos frequente[45], pelo que a norma será, automaticamente, mais restritiva, uma vez que a CRP determina como garantia fundamental o controlo das ingerências em direitos fundamentais por um juiz, portanto, só são suscetíveis de serem praticados por outras autoridades judiciárias os atos que não afetem diretamente tais direitos fundamentais (cf. art. 32.º, n.º 4, CRP).

O CPP, prevendo que "sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho" a apreensão de cartas ou outro tipo de correspondência (art. 179.º, n.º 1), e indo de encontro à doutrina e à jurisprudência, considera-se que a apreensão de correspondência comum prevista no código em questão "só pode ser ordenada por um juiz, por força do artigo 32.º, n.º 4 da Constituição"[46], pelo que, interpretando de acordo com a CRP, apenas o juiz possui a faculdade de decidir que se permite a intervenção em direitos fundamentais do sigilo das correspondências e das telecomunicações, estando em causa matéria de reserva de juiz autorizar ou ordenar a apreensão[47].

Nas palavras de João Conde Correia "ao contrário das apreensões em geral que podem ser decretadas pelo juiz, pelo MP (art. 178.º, n.º 3) ou, até, em certos casos mais limitados, pelos próprios OPC (art. 178.º, n.º 4), exige-se aqui a intervenção judicial prévia"[48]. O legislador considerou que os direitos fundamentais em causa (direito de propriedade, sigilo da correspondência, vida privada) eram demasiados importantes e que o grau de restrição seria demasiado elevado para poder confiar na decisão de outra entidade, ainda que sujeita a eventual validação judicial oficiosa.

Será importante ter em conta que o regime de apreensão de correspondência previsto no CPP consiste na "retirada do circuito normal do correio[49] (o que implica que o processo comunicacional esteja em curso) do suporte através do qual se efetua uma comunicação postal ou telegráfica, impedindo que chegue ao seu destinatário"[50], pelo que este regime de apreensão de correspondência possa restringir o direito à inviolabilidade da correspondência.

Porquanto, em casos excecionais, em que a demora na abertura de correspondência pode resultar na perda de informações frutuosas e essenciais para a

[45] *Idem*, p. 640.
[46] ALBUQUERQUE, 2011, p. 509; CANOTILHO, MOREIRA, 2007, p. 544.
[47] ANTUNES, 2021, p. 136.
[48] CORREIA, 2019, p. 647.
[49] ALBUQUERQUE, 2011, p. 509.
[50] NUNES, 2021, p. 335.

investigação de um crime, o juiz pode autorizar a sua abertura imediata pelos OPC, em contexto de medidas cautelares e de polícia, segundo o disposto no art. 252.º, n.º 2, do CPP, sendo que o juiz detém o dever de validar a ordem por despacho fundamentado no prazo de 48 horas.

3.2. Apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17.º da LCC)

Diversamente da apreensão de correspondência regulada no CPP, a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante, regulada no art. 17.º da LCC, aplica-se não à obtenção em tempo real, mas sim à obtenção de correio "que já foi recebido pelo destinatário (ou que ainda não foi ou já fora remetido pelo remetente) e que se encontra armazenado no sistema informático que foi legitimamente acedido pelas autoridades (...)"[51].

O conceito de correio eletrónico, segundo Rui Cardoso, define-se como "qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha" [52]. Contudo, atualmente encontramos outros tipos de comunicações eletrónicas (as tais comunicações de natureza semelhante) como as SMS, EMS, MMS, conversas no *Messenger, Whatsapp, Viber, Skype*, etc.[53]

Perante isto, o legislador consagrou na LCC diversos meios de obtenção de prova que permitem obter o conhecimento e o conteúdo deste tipo de comunicações, como é o caso do art. 17.º desta lei em questão.

A origem deste artigo encontra-se na Proposta de Lei n.º 289/X/4ª, tendo ele a mesma redação que o art. 19.º desta Proposta. A leitura da Exposição de Motivos da Proposta demonstra que o Governo, reconhece a "desadequação da ordem jurídica nacional às novas realidades a implementar", pelo que não tencionou fazer apenas uma extensão do regime das buscas e apreensões previsto no CPP à prova digital, mas sim proceder a uma adaptação desse regime, "a forma como a busca e a apreensão estão descritas no CPP exigiam alguma adequação a estas novas realidades"[54].

[51] *Idem,* p. 336.
[52] CARDOSO, 2018, p. 181 e ss.
[53] NUNES, 2021, p. 332.
[54] CARDOSO, 2018, pp. 169 e 170.

Assim, com o art. 17.º, nasce um regime especial de apreensão de dados que tem como objetivo permitir, em circunstâncias específicas, apreender o correio eletrónico e outros registos de comunicação de natureza semelhante, sendo que estas normas têm como tónica comum pretenderem adaptar para o ambiente digital e dos sistemas informáticos as habituais diligências de busca e apreensão[55].

Como já foi referido, o regime previsto neste art. 17.º da LCC tem gerado dificuldades de compatibilização com o disposto no CPP, pelo que se colocam alguns problemas. Um dos problemas tem que ver com o pressuposto relativo ao crime em causa (crime punível com pena de prisão superior, no seu máximo, a 3 anos), o problema coloca-se, desde logo, no facto de alguns dos tipos legais previstos na LCC não serem puníveis com penas de prisão superiores a 3 anos.

Nas normas relativas à interceção de comunicações e à admissibilidade de ações encobertas, o legislador refere expressamente que tais meios processuais podem ser utilizados em processos relativos a crimes previstos na LCC (art. 18.º, n.º 1, alínea a), e art. 19.º, n.º 1, alínea a)) e noutros processos por crimes que integrem o catálogo de crimes referido em cada uma das normas (art. 18.º, n.º 1, alínea b), e art. 19.º, n.º 1, alínea b)).

Conclui-se, então, que foi opção do legislador permitir a apreensão de correio eletrónico e registos de comunicações de natureza semelhante sem a limitação resultante de o crime ser punível com pena de prisão superior a 3 anos, pelo que se permite a utilização deste meio de obtenção de prova em processos relativos aos crimes previstos na própria LCC (como, aliás, acontece também com a interceção de comunicações e as ações encobertas).

Outra questão que se tem colocado está relacionada com a exigência de despacho judicial prévio, que autorize ou ordene a apreensão de mensagens de correio eletrónico, bem como saber se o juiz deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico apreendidas. Contudo, estes problemas serão abordados mais adiante.

3.2.1. Mensagens de correio eletrónico abertas e não abertas

Atualmente, um tema que gerou enorme discussão relaciona-se com o facto de saber se a analogia estabelecida com o regime que regula a apreensão de correspondência

[55] VERDELHO, 2019, p. 741.

deve aplicar-se a todo o correio eletrónico, ou apenas às situações em que este não foi ainda lido pelo destinatário, aplicando-se ao correio lido o regime da simples apreensão de documentos.

Até à aprovação da LCC, seriam diversas as posições que afastavam qualquer paridade entre as mensagens de correio eletrónico recebidas num sistema informático e o conceito tradicional de correspondência ou carta.

Pedro Verdelho defendia que, quanto às mensagens recebidas, mas ainda não lidas, seria compreensível conceder o mesmo tratamento que o correio físico contido em envelopes não abertos (o dito correio tradicional), pelo que a sua apreensão só poderia ocorrer nos casos previstos do art. 179.º do CPP. Porém, em relação às mensagens recebidas e já lidas, considerando que já foram, justamente, abertas, lidas e guardadas no computador a que se destinavam, não deveriam ter mais proteção do que as cartas em papel recebidas, abertas e guardadas numa gaveta ou arquivo, portanto, não mereciam a mesma proteção em relação às outras, no momento da sua apreensão[56].

Questiona-se se, a partir do momento da leitura, a mensagem de correio eletrónico ou de natureza semelhante, não passa a ser um documento eletrónico igual a qualquer outro, "(...) sujeitando-se ao regime correspondente àquele a que ficam sujeitos os documentos que o visado cria e arquiva no seu computador"[57].

Como é possível observar, o art. 17.º da LCC não faz qualquer distinção entre mensagens de correio eletrónico ou de natureza semelhante abertas e não abertas, sendo que o aberto e não aberto (ou lido e não lido), não é uma forma banal de proteção do conteúdo da mensagem, contrariamente ao que sucede com os envelopes no correio corpóreo, "Não são envelopes ou invólucros das mensagens, mas simples filtros que o utilizador por definir (de acordo com as suas preferências ou critérios), para mais facilmente gerir o volume de mensagens de correio eletrónico recebidas"[58].

Ora, no sentido do paralelismo entre correio eletrónico lido pelo destinatário e simples documentos, Manuel da Costa Andrade defende que "depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito. E, como tal, sujeito ao

[56] VERDELHO, 2004, p. 158.
[57] Ac. do TC nº. 687/2021, p. 10.
[58] CARDOSO, 2018, pp. 186-187.

mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado."[59].

Paulo Dá Mesquita segue a mesma linha de pensamento, assegurando que apesar da redação pouco clara do art. 17.º, a remissão para as normas do CPP faz parecer que "(...)a mesma reconduz o intérprete à teleologia do regime processual sobre a apreensão de correspondência, pelo que não são objeto da sua tutela especial, nomeadamente, mensagens de correio eletrónico já acedidas pelo destinatário"[60].

Contudo, nunca será uma ideia consensual, já que na opinião de Rita Castanheira Neves que, sendo a favor de uma maior garantia do correio eletrónico já lido, entende que "a Lei do Cibercrime consagra uma distinção de regime para o e-mail armazenado, que nem equipara à proteção da interceção do e-mail enquanto comunicação, nem à (falta de) proteção dos normais escritos.(...) O que a Lei n.º 109/2009 faz é reconhecer ao correio eletrónico apenas dois momentos, com separação entre um e outro desde a leitura do e-mail pelo destinatário, mas conferindo, ao mesmo tempo, proteção acrescida ao segundo momento, de armazenamento, fazendo coincidir os requisitos previstos para o regime da correspondência"[61].

Acontece que a matéria em questão contende com direitos fundamentais, mais concretamente com o direito à inviolabilidade da correspondência e das telecomunicações.[62]

A CRP, no seu art. 26.º, n.º 1, reconhece os direitos à identidade pessoal, ao desenvolvimento da personalidade e à reserva da intimidade da vida privada e familiar. Já no seu art. 34.º, n.º 4, consagra que "(...) o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis" (n.º 1) e que "É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal".

Para autores como Gomes Canotilho e Vital Moreira, "O conteúdo do direito ao sigilo da correspondência e de outros meios de comunicação privada (n.º 1 e 4) abrange toda a espécie de correspondência de pessoa a pessoa (cartas postais, impressos), cobrindo mesmo as hipóteses de encomendas que não contêm qualquer comunicação escrita, e todas as telecomunicações (telefone, telegrama, telefax, etc.)" [63]. Ademais, no âmbito do

[59] ANDRADE, 2012, ponto 27.
[60] MESQUITA, 2010, p. 118.
[61] NEVES, 2011, pp. 276-277.
[62] CARDOSO, 2018, p. 175.
[63] CANOTILHO, MOREIRA, 2007, p. 544.

art. 34.º insere-se o correio eletrónico, uma vez que o segredo da correspondência abrange as correspondências mantidas por via das telecomunicações, pelo que, na opinião destes autores, todo o tipo de correspondência merece tutela jurisdicional.

Por outro lado, seguindo Manuel da Costa Andrade, a tutela do sigilo das telecomunicações está diretamente ligada ao processamento da comunicação sob o domínio da empresa provedora do serviço de telecomunicações, sendo que esta tutela "só existe enquanto dura o processo dinâmico de transmissão, isto é, até ao momento em que a comunicação entra na esfera de domínio do destinatário. Vale dizer, até ao momento em que ela é recebida e lida pelo destinatário e, neste sentido, termina o processo de telecomunicação à distância. Assim, depois de recebido, lido e guardado no computador do destinatário, um email deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito"[64].

Acontece que, no que respeita às mensagens de correio eletrónico ou de natureza semelhante, é muito difícil ou mesmo impossível determinar quando é que termina a comunicação e se a mensagem já foi ou não aberta/lida. Porém, não significa que não existam direitos fundamentais dignos de tutela.

No Ac. 403/2015 do TC, foram idealizadas marcantes considerações sobre o acesso aos dados das comunicações (mesmo depois de terminadas), constatando que tal colide com o direito à autodeterminação comunicativa, protegido no art. 34.º da CRP, que serve para defender vários bens jurídico-constitucionais, tais como o direito ao desenvolvimento da personalidade e o direito à reserva da intimidade da vida privada e, também, para proteger "a esfera pessoal perante as ingerências públicas ou privadas, ou seja, o interesse das pessoas que comunicam em impedir ou em controlar a tomada de conhecimento, a divulgação e circulação do conteúdo e circunstâncias da comunicação"[65].

João Correia, em conformidade com Manuel da Costa Andrade, Rita Castanheira Neves e Pedro Verdelho, faz uma distinção entre *e-mails* lidos e não lidos (relacionando-se com a distinção entre correspondência aberta e não aberta), muito embora a LCC não a faça. Assim, conforme dispõe Rui Cardoso, "a correspondência merece tutela desde o momento do envio, fechada, até ao momento da abertura pelo destinatário"[66], pois, tal

[64] ANDRADE, 2009, p. 158-159.

[65] https://dre.pt/dre/detalhe/acordao-tribunal-constitucional/403-2015-70300353, acedido a 04/03/2002.

[66] CARDOSO, 2018, p. 56-57.

como assegura Manuel da Costa Andrade, "é precisamente este facto – estar fechada – que define a fronteira da tutela penal do sigilo de correspondência e dos escritos em geral"[67]. Daí que a correspondência, depois da sua abertura, fica sujeita ao regime geral de apreensão, previsto no art. 178.º do CPP.

Desta forma, o regime da proteção do sigilo da correspondência física do CPP só vale enquanto a mesma estiver em trânsito e ainda não tiver sido aberta pelo destinatário, pois "a partir desse momento (conclusão efetiva do processo de transmissão) o destinatário dispõe dos meios necessários a evitar a intromissão estadual. Ele já não está vulnerável, sujeito às falhas de reserva do operador ou à curiosidade estadual"[68].

Destarte, os peritos informáticos demonstram que se pode marcar uma mensagem como lida ou não lida com bastante facilidade, pelo que esta distinção entre correio eletrónico lido e não lido, bem como as diferentes formas de tratamento defendidas por João Correia, Manuel da Costa Andrade, Rita Castanheira Neves, Pedro Verdelho e Paulo Dá Mesquita já não fazem grande sentido.

Assim, pactuamos com Rui Cardoso quando alega que alguns prestadores de serviços de correio eletrónico "(...)continuam a ter regimes de lido/não lido, mas que, contrariamente ao que sucede com a correspondência corpórea, podem ser facilmente alteráveis (e infinitamente) pelo utilizador, com um clique. O correio eletrónico pode ser arquivado pelo destinatário sem ser lido; pode ser arquivado juntamente com mensagens enviadas e até rascunhos de mensagens eventualmente a enviar"[69].

Por conseguinte, a doutrina tem evoluído para uma posição mais consensual, desconsiderando a distinção entre correio eletrónico lido e não lido pelo destinatário, com suporte na letra do artigo 17.º da LCC. "A consagração de um regime jurídico único, especificamente desenhado para a figura do correio eletrónico, permite, aliás, ultrapassar incongruências e antinomias que resultariam de um tratamento jurídico diferenciado entre as mensagens guardadas no sistema informático do visado e as mensagens armazenadas em nuvem, ou no sistema informático do prestador do serviço"[70].

Deste modo, estamos a caminhar no sentido de uma disciplina de apreensão de correio eletrónico em processo penal tendencialmente unitária, que permite encarar as questões colocadas por tal realidade, levando em consideração os direitos fundamentais

[67] ANDRADE, 2012, p. 758.
[68] CORREIA, 2014, p. 41.
[69] CARDOSO, 2018, p. 187.
[70] Ac. do TC n.º 687/2021, p. 11

constitucionalmente tutelados (suprarreferidos), contribuindo para ultrapassar as divergências provocados pelo enquadramento normativo dos *e-mails* nas fases e no tempo em que foram guardados na conta, tanto na fase intermédia em que a mensagem não foi ainda aberta ou lida pelo destinatário, como na fase final, em que depois de aberto e lido, o *e-mail* é depositado no servidor, ao qual só é possível aceder através da *Internet*, isto é, através de um ato de telecomunicação[71].

"Por esta razão, e atendendo igualmente aos bens jurídico-constitucionais e aos direitos fundamentais em causa, bem como à necessidade de uma compreensão atualista da tutela jusconstitucional conferida pela CRP nesta matéria, atender-se-á ao regime jurídico de apreensão de correio eletrónico sem proceder a este tipo de distinções"[72].

3.3. As competências do JIC e do MP relativas à apreensão de correio eletrónico e registos de comunicações de natureza semelhante

A reserva de juiz é a garantia de vários direitos fundamentais, recebendo atenção do constituinte português ao contemplar que "toda a instrução é da competência de um juiz, o qual pode, nos termos da lei, delegar noutras entidades a prática dos atos instrutórios que se não prendam diretamente com os direitos fundamentais" (art. 32.º, n.º 4, CRP). Assim, as reservas de juiz "traduzem-se em normas legais de competência que conferem a um juiz o poder exclusivo e obrigatório para decretar medidas de ingerências nos direitos individuais"[73].

Ora, o instituto da reserva de juiz pressupõe que momento de pronuncia do juiz deve ser, por regra, em momento prévio ao ato ou durante a execução do mesmo, e não depois[74]. Contudo, podem ser deixadas à competência do MP "(...) todas as medidas de ingerência que não afetassem direitos fundamentais, reservando-se para a autorização do juiz apenas as medidas que atingissem diretamente aqueles direitos"[75].

Tal como foi referido, duas grandes questões que se têm colocado estão relacionadas com a exigência de despacho judicial prévio, que autorize ou ordene a apreensão de mensagens de correio eletrónico, bem como saber se o juiz deve ser a

[71] ANDRADE, 2012, ponto 28.
[72] Ac. do TC n.º 687/2021, p. 11.
[73] MATA-MOUROS, 2011, p. 53.
[74] *Idem.*
[75] *Idem.*

primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico apreendidas.

Ora, o problema surge quando o art. 17.º da LCC remete para a aplicação correspondente do regime da apreensão de correspondência do CPP, regulada nos artigos 179.º e 252.º. Ambos os diplomas dispõem que o juiz pode autorizar (o requerimento do MP no âmbito do inquérito) ou ordenar (quando o próprio juiz autoriza) por despacho a apreensão de correio eletrónico (LCC) ou apreensão de correspondência (CPP), não referindo se o despacho deve ser ou não prévio.

Pedro Verdelho[76], assume que o MP e os OPC's possuem a faculdade de ordenar ou autorizar uma apreensão provisória ou cautelar das mensagens de correio eletrónico, que será submetida e validada pelo juiz, não se exigindo uma prévia decisão judicial para a apreensão.

Além do mais, na prática, na realização de uma busca, não se prevê quantos computadores serão encontrados, bem como numa eventual pesquisa informática não se prevê se serão encontrados *e-mails*, muito menos se esses *e-mails* serão de interesse para a descoberta da verdade. Assim, de forma a não violar os direitos fundamentais, tais como a reserva da intimidade da vida privada (art. 26.º, n.º 1, CRP) e a inviolabilidade e o sigilo da correspondência (art. 34.º, n.º 1 e 4, CRP), deve haver despacho prévio do juiz (cf. art. 32.º, n.º 4 e 8, CRP e art. 179.º, n.º 1, alínea c) e n.º 3, CPP)[77].

A lei não é expressa, mas é clara, uma vez que assume que é possível proceder-se a uma apreensão de mensagens de correio eletrónico mesmo que não tenha havido nenhuma anterior ordem judicial nesse sentido. Será esta a ideia que se retira do art. 17º da LCC, quando prevê a possibilidade de o juiz autorizar a apreensão de mensagens que se mostrem de grande importância para a descoberta da verdade, "se as mesmas forem descobertas ou encontradas no decurso de uma pesquisa informática ou outro acesso ilegítimo a um sistema informático."[78]. Neste caso, o despacho judicial do juiz deverá ser subsequente à chegada das mensagens ao conhecimento de quem está a orientar a investigação. Esta apreensão é provisória uma vez que, caso o juiz entenda dever autorizar a apreensão, a mensagem em causa será efetivamente apreendida e junta ao processo.

[76] VERDELHO, 2009, pp. 743-744.
[77] *Idem.*
[78] VERDELHO, 2019, p. 743.

Caso contrário, "então a apreensão não se mantém, devendo o suporte das mensagens em causa ser devolvido ou, se a apreensão tiver sido feita por cópia, destruído"[79].

Este regime de apreensão permite que o procedimento seja mais flexível e célere pois, de facto, as mensagens serão encontradas e apreendidas no decurso da pesquisa, sendo fácil perceber que não é possível antecipar que, numa busca, se irá encontrar um computador, muito menos saber se esse computador contenha mensagens de correio eletrónico ou de natureza semelhante que tenham interesse para a investigação.

Entende-se que legislador não foi muito claro sobre este aspeto. No entanto, não parece viável nenhuma outra interpretação da lei, pois de outra forma, optar-se-ia por uma solução que exigiria a verificação, pelo juiz, de todas as mensagens de correio eletrónico, de todos os computadores que fossem encontrados durante as investigações[80]. Esta solução seria impossível tendo em conta a quantidade colossal de computadores que nos dias de hoje se apreendem.

Deverá, então, entender-se, segundo Pedro Verdelho, que a lei permite que se faça uma apreensão provisória de mensagens de correio eletrónico, no âmbito de pesquisas informáticas realizadas, por exemplo, com autorização do MP, sendo depois tais mensagens presentes ao juiz, para que este ordene a respetiva apreensão e junção ao processo. Por essa compreensão, não se exigiria a análise imediata e anterior do juiz.

Contrariamente a esta ideia, defende João Correia que "Segundo o BVerfG, a infiltração secreta em sistemas informáticos alheios, para efeitos de monitorização ou de leitura de dados, será constitucionalmente admissível, mediante prévia autorização judicial, em caso de perigo concreto para bens jurídicos individuais como a vida, o corpo ou a liberdade ou para interesses coletivos, cuja ameaça afete os fundamentos ou a sobrevivência do Estado de direito ou da própria existência humana"[81].

Portanto, o legislador não tendo delimitado o âmbito dessa aplicação correspondentemente, será da competência do juiz essa delimitação, sendo um dever o juiz intervir sempre que estiverem em causa direitos fundamentais, conforme artigo 32.º, n.º 4 da CRP.

Com efeito, pode-se afirmar que o direito da inviolabilidade da correspondência possui como garantia a necessidade de prévio despacho judicial, para que sofra uma eventual restrição.

---

[79] *Idem.*
[80] VERDELHO, 2019, p. 744.
[81] CORREIA, 2014, p. 44.

Acontece que a LCC não sendo precisa sobre o facto de dever ser ou não o juiz o primeiro a ter acesso ao conteúdo dos *e-mails* apreendidos, será necessário ter em conta a análise da jurisprudência sobre o assunto. O Ac. do TRL de 11 de janeiro de 2011 determina que o regime geral do CPP sobre apreensão de correspondência deve ser aplicado na sua totalidade, sem redução do seu âmbito à apreensão de correio eletrónico, em conformidade com o que dispõe o art. 17.º da LCC.

Em contraposição, Rui Cardoso considera que "o art. 17º determina a correspondente aplicação do regime de apreensão de correspondência do CPP, não a aplicação integral. Esta só deve ser feita naquilo que não contrariar o já previsto na própria LCC (...)"[82], pois foi a intenção do legislador adaptar a busca e a apreensão previstas no CPP às novas realidades.

Atentando a posição do Ac. do TRL, o art. 179.º, n.º 3 do CPP deve ver a sua aplicação estendida ao conteúdo do correio eletrónico *"*(...) já convertido em ficheiro legível, o que constitui ato da competência exclusiva do juiz de instrução criminal, nos termos do art. 268º, nº1, al. d, CPP, (...) constituindo a sua violação nulidade expressa absoluta e que se reconduz, a final, ao regime de proibição de prova. A tudo isto acresce que a falta de exame da correspondência pelo juiz constitui uma nulidade prevista no art. 120º, nº2, al. d, CPP porque se trata de um ato processual legalmente obrigatório"[83], pelo que deve ser o JIC que tiver autorizado ou ordenado a apreensão dos *e-mails* também o primeiro a tomar conhecimento do seu conteúdo, sob pena de nulidade e produção de prova proibida que não pode ser valorada.

Porém, é feita uma ressalva em caso de urgência, previsto no art. 252.º, n.º 2 e 3, do CPP, declarando que no caso da perda de informações úteis à investigação de um crime ou em caso de demora, o juiz pode autorizar a abertura imediata de correspondência (e, também, de correio eletrónico) pelo órgão de polícia criminal, sendo que o órgão de polícia criminal pode ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, devendo a ordem policial ser validada pelo juiz no prazo de 48 horas, sob pena de devolução ao destinatário ou caso a ordem não seja validada.

[82] CARDOSO, 2018, p. 66.

[83] http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument, ponto 7, acedido a 04/03/2022.

Percebe-se que, mesmo em situação excecional, o juiz deve autorizar que o OPC possa ler a correspondência antes dele, bem como deve autorizar, por despacho fundamentado, uma eventual ordem desse órgão de suspensão da remessa. Esta participação do juiz destaca seu papel de garante dos direitos fundamentais, conforme art. 32.º, n.º 4, CRP, o que não poderia ser diferente no âmbito da apreensão de correio eletrónico.

Acórdão mais recente, mas seguindo o mesmo sentido será o Ac. do TRL de 6 de fevereiro de 2018[84], reiterando o posicionamento do acórdão anterior, indicando que esta questão vem sendo decidida no mesmo sentido há alguns anos pelo TRL.

Rui Cardoso[85] invoca a violação da estrutura acusatória do processo penal (art. 32.º, n.º 5, CRP), porquanto que exigindo que seja o juiz a ler os *e-mails* e a selecionar o que inclui no processo, seria o mesmo a determinar as provas que se incluem no processo, o que não seria função do juiz da instrução, mas do MP (titular do inquérito). Haveria, assim, usurpação de competências. No entanto, apesar de o MP ser responsável pelas investigações e com a faculdade de decidir quais as provas mais relevantes para o processo, percebe-se que o juiz também deve ter amplo conhecimento da causa, sendo igualmente apto a realizar tal função. Além disso, o mesmo ocorre quando há apreensão de correspondência tradicional do art. 179.º, CPP, uma vez que a correspondência é entregue ao juiz, sendo ele a decidir quais provas se devem incluir ou não no processo (art. 179.º, n.º 3, CPP). Dessa forma, não se verifica nenhum impedimento para que seja o juiz da instrução o primeiro a ler o conteúdo dos *e-mails* apreendidos, indo de encontro com a posição dominante dos acórdãos suprarreferidos, bem como com as disposições do CPP.

Pedro Verdelho assume que a lei não foi clara nesse ponto, portanto, nas palavras deste autor, "estaria a optar-se por uma solução processual inviável, que exigiria a verificação, pelo juiz, de todas as mensagens de correio eletrónico, em todos os computadores que fossem encontrados no decurso de pesquisas."[86]. Desta forma, não se exige que seja o juiz o primeiro a ter conhecimento de todas as mensagens como acontece com o correio físico, a letra da lei aponta antes para a possibilidade de quem procede à pesquisa encaminhar para o juiz mensagens concretas, com relevância para o caso

[84] http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument, acedido a 04/03/2022.

[85] CARDOSO, 2018, p. 68.

[86] VERDELHO, 2009, p. 744.

concreto, decidindo, posteriormente, se apreenderá ou não. Pensamento que vai de encontro com a opinião de Duarte Rodrigues Nunes[87], seguindo a decisão do TRG quando proferiu o entendimento de que o MP pode obter acesso ao teor do conteúdo das conversas e apreender um SMS, antes da decisão do juiz da instrução[88].

Caso se considere este entendimento o mais adequado, estar-se-ia a permitir que um maior número de pessoas tivesse acesso aos dados do visado, pelo que resultava numa maior vulnerabilidade dos seus direitos fundamentais de sigilo das comunicações, bem como da reserva da intimidade de sua vida privada, contrariando-se o art. 32.º, n.º 4 da CRP, que dispõe que o juiz pode delegar em outras entidades a prática de atos instrutórios desde que não se prendam diretamente com os direitos fundamentais.

Já na opinião de Paulo Dá Mesquita[89] e Rita Castanheira Neves[90] não faz sentido assegurar que é inviável o juiz ser o primeiro a ler os múltiplos *e-mails*, selecionando os que são ou não relevantes para processo, mas que já seja viável fazê-lo quando se trata de correio físico. Assim, como a regra do art. 179.º, n.º 3, CPP não contraria a LCC sendo omissa neste âmbito, pode e deve ser o juiz o primeiro a ter conhecimento do conteúdo dos correios eletrónicos apreendidos.

Com efeito, a ponderação deve ser realizada por um juiz e, citando Jorge Figueiredo Dias, "É através desta ponderação e da justa decisão do conflito que se exclui a possibilidade de abuso de poder – da parte do próprio Estado ou dos órgãos a eles subordinados – e se põe a força da sociedade ao serviço e sob o controle do direito; o que traduz só, afinal, aquela limitação do poder do Estado pela possibilidade de livre realização da personalidade ética do homem que constitui o mais autêntico critério de um verdadeiro Estado-de-direito"[91].

Conclui-se, portanto, que subsiste a necessidade de um despacho prévio judicial emanado por um juiz, para concretizar qualquer ingerência no sigilo de correspondência eletrónica.

[87] NUNES, pp. 347 e ss.

[88] http://www.dgsi.pt/jtrg.nsf/c3fb530030ea1c61802568d9005cd5bb/6aa96edf91e899b2802578a00054631f?OpenDocument, acedido a 04/03/2022.

[89] MESQUITA, 2010, pp. 117 e ss.

[90] NEVES, 2011, pp. 274-275.

[91] DIAS, 2004, p. 59.

4. Proposta de alteração do artigo 17.º (Decreto n.º 167/XIV) e Acórdão do TC sobre a apreensão do correio eletrónico (Ac. n.º 687/2021)

De acordo com o art. 17.º da LCC, aquando do decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontradas mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar a apreensão dos que se aparentem ser de grande interesse para a descoberta da verdade ou para a prova, sendo aplicado, correspondentemente, o regime da apreensão de correspondência previsto no CPP.

Assim, o Decreto n.º 167/XIV teve como propósito clarificar o modelo de apreensão de correio eletrónico e da respetiva validação judicial. Em particular, pretendeu alterar o disposto no art. 17.º da LCC relativamente à questão da autorização pelo juiz, através de despacho prévio, de apreensão de correio eletrónico e registos de comunicações de natureza semelhante, passando a não ser necessário existir o tal despacho para a autoridade judiciária proceder à apreensão.

Por um lado, visa esclarecer que a apreensão de mensagens de correio eletrónico ou de registos de comunicações de natureza semelhante está sujeita a um regime autónomo, que vigora em paralelo com o regime da apreensão de correspondência previsto no CPP. Por outro lado, visa esclarecer que a apreensão de mensagens de correio eletrónico ou de natureza semelhante guardadas num determinado dispositivo, embora incidindo sobre dados informáticos de conteúdo especial, não é tecnicamente diferente da apreensão de outro tipo de dados informáticos.

Assim, deve o MP, após a análise do respetivo conteúdo, apresentar ao juiz as mensagens e registos "cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto"[92].

Esta solução procura replicar, no domínio das mensagens de correio eletrónico ou de natureza similar, a solução presentemente aplicável aos dados e documentos informáticos cujo conteúdo possa revelar dados pessoais ou íntimos, pondo em causa a

92 https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c6379395953565a4d5a5763765247396a6457316c626e52766330466a64476c32615752685a47565159584a735957316c626e52686369396d4e6a566b5a5751795a6930355a5459354c54526c4d3249744f444d785a533169596a4d784d6a4e6b5a54597a4d5449755a47396a65413d3d&fich=f65ded2f-9e69-4e3b-831e-bb3123de6312.docx&Inline=true, acedido a 04/03/2022.

privacidade do respetivo titular ou de terceiro. Acontece que o teor deste Decreto tem gerado bastantes conflitos jurisprudenciais.

Com o Acórdão n.º 687/2021, o TC pronunciou-se pela primeira vez sobre o regime de apreensão do correio eletrónico, tendo apreciado o Decreto n.º 167/XIV da AR, na parte em que alterava o art. 17.º da LCC. Por unanimidade, o TC pronunciou-se pela "inconstitucionalidade das normas constantes do seu artigo 5.º, na parte em que altera o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, por violação das normas constantes dos artigos 26.º, n.º 1, 34.º, n.º 1, 35.º, n.º 1 e 4, 32.º, n.º 4, e 18.º, n.º 2, da Constituição da República Portuguesa".

Na fundamentação do Ac., o TC evidencia alguns problemas sobre o regime vigente da prova digital, em especial sobre a apreensão de dados informáticos e, mais ainda, sobre o regime vigente de apreensão de dados informáticos e a divisão de competências nele feita entre MP e JIC na fase de inquérito.

Relativamente à questão controversa da exigência prévia (ou não) de despacho judicial que decreta a apreensão de mensagens de correio eletrónico, Sónia Fidalgo[93] afirma que as respostas têm sido diversas, pois há quem defenda que a apreensão só pode ser feita na sequência de um despacho judicial, porém, também há quem entenda que a lei não é expressa a este propósito, permitindo que se proceda a uma apreensão cautelar ou provisória de mensagens de correio eletrónico mesmo que não tenha havido um despacho judicial anterior.

Na ideia de Rui Cardoso, o Ac. evidencia o entendimento de que a apreensão de correio eletrónico deve seguir o regime da apreensão de correio físico. Esse entendimento é manifesto na leitura do art. 17.º ao remeter para o disposto no art. 179.º do CPP, que seria substituída, na nova versão em causa, por uma previsão de aplicação subsidiária e com as necessárias adaptações do disposto naquela norma do CPP. "(...) a aplicação correspondente do regime do artigo 179.º do CPP deve hoje ser exactamente essa: de aplicação subsidiária e com as necessárias adaptações. Só se pode aplicar esse regime naquilo que não estiver especialmente previsto na LCC: a remissão para o CPP não pode sobrepor-se ao regime especial de prova electrónica previsto na LCC."[94].

De facto, no Ac. em questão, o TC começa por afirmar que a restrição dos direitos fundamentais em causa é possível, nos termos do art. 34.º, n.º 4 da CRP, uma vez que o legislador constituinte "(...) entendeu que os valores jurídico-constitucionais em causa em

[93] FIDALGO, 2019, p. 157.
[94] CARDOSO, 2021, p. 148.

sede de processo penal o justificam – mesmo tratando-se de direitos aos quais se atribuiu uma protecção de tal forma reforçada que não cedem noutras situações (...)" (ponto 41, 4§). Porém, posteriormente conclui que "(...) não se vê como possa afirmar-se que as normas questionadas satisfaçam as exigências de excecionalidade, necessidade e proporcionalidade que se impõem às leis restritivas de direitos fundamentais, por força do artigo 18.º, n.º 2, da CRP. Na verdade, não se veem razões para afastar a intervenção prévia do Juiz de Instrução Criminal, em fase de inquérito, no que respeita aos atos de apreensão do correio eletrónico ou similar (...)" (ponto 44, 1§).

Ademais, adiante conclui ainda que a norma em questão "(...) é inconstitucional por violação dos direitos fundamentais à inviolabilidade da correspondência e das comunicações (consagrado no artigo 34.º, n.º 1, da CRP), à proteção dos dados pessoais no âmbito da utilização da informática (nos termos do artigo 35.º, n.º 1 e 4, da CRP), enquanto refrações específicas do direito à reserva de intimidade da vida privada, (consagrado no artigo 26.º, n.º 1, da Constituição), em conjugação com o princípio da proporcionalidade (nos termos do artigo 18.º, n.º 2, da CRP) e com as garantias constitucionais de defesa em processo penal (previstas no artigo 32.º, n.º 4, da Lei Fundamental)" (ponto 46).

Rui Cardoso afirma no sentido de que a exigência de proporcionalidade e a potencial ofensa aos direitos fundamentais, "nada têm que ver com a entidade que decide o recurso ao meio de obtenção de prova/a utilização do meio de prova; não se confundem, enfim, com a reserva de juiz prevista no n.º 4 do artigo 32.º"[95]. Estando em causa prováveis intromissões em direitos fundamentais, a intervenção reservada ao JIC no inquérito deverá "(...) consistir numa intervenção prévia, devendo ser vista como excecional a intervenção do juiz que surge apenas após o início da execução da medida."[96].

Acontece que a função do juiz será sempre de defesa dos direitos, liberdades e garantias dos cidadãos legalmente protegidos, pelo que, estando em causa direitos fundamentais aquando de qualquer apreensão, deve existir uma autorização prévia judicial. Além do mais, o art. 34.º da CRP, no seu n.º 4, dispõe que "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação...", tratando-se de uma refração do direito da reserva à intimidade da vida privada consagrado no art. 26º, n.º 1 da CRP.

[95] *Idem*, p. 154.
[96] *Idem.*

Outra questão que se tem colocado é a de saber se o juiz deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico apreendidas.

Ao entender-se que o JIC deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens apreendidas pode pôr em causa a própria coerência do sistema de tutela de direitos, na medida em que nos casos de interceção de comunicações (art. 18.º da LCC) é permitido aos OPC's e ao MP que sejam os primeiros a tomar conhecimento do conteúdo das comunicações (art. 18.º, n.º 4, LCC e art. 188.º, n.º 1 a 4, do CPP)[97].

Não obstante, na opinião de Rui Cardoso, a exigência de que seja o JIC o primeiro a conhecer o conteúdo das mensagens apreendidas e, consequentemente, a selecionar as que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, viola a estrutura acusatória do processo penal. Porém, é de referir que um processo onde vigore o princípio da investigação desenrola-se de forma diferente, uma vez que o JIC tem a faculdade de "(...) investigar e esclarecer oficiosamente o facto submetido ou a submeter a julgamento (...)"[98], sendo compatível com os princípios da legalidade da prova e da estrutura acusatória do processo, pelo que não há uma violação da referida estrutura acusatória.

A nossa jurisprudência não tem sido sensível a estes argumentos, entendendo que em causa está o direito à privacidade e ao sigilo da correspondência eletrónica (art. 26.º, n.º 1, e art. 34.º, n.º 4, da CRP), considerando que a remissão do art. 17.º da LCC que se faz para o regime de apreensão de correspondência previsto no CPP abrange o disposto no n.º 3 do art. 179.º. Os tribunais têm entendido que o juiz que autoriza ou ordena a diligência deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens apreendidas[99], uma vez que o regime previsto no art. 179.º do CPP dispõe que as apreensões de correspondência tradicional tanto necessitam de despacho judicial (art. 179.º, n.º 1), como dispõe que o juiz será a primeira pessoa a tomar conhecimento do conteúdo da correspondência, o que constitui ato da competência exclusiva do JIC por força do art. 268.º, n.º 1, alínea d), do CPP.

Ora, aplicando o regime do art. 179.º ao regime de apreensão de correio eletrónico previsto no art. 17.º da LCC, significa que o regime previsto no CPP se estende ao

[97] CARDOSO, 2018, p. 197 e ss.
[98] ANTUNES, 2021, p. 186.
[99] Neste sentido, os Ac. do TRL, processo n.º 5412/08.9TDLSB-A.L1-5, de 11-01-2011; Ac. do TRL, processo n.º 184/12.5TELSB-R.L1-3, de 27-01-2021; e Ac. do TRL, processo n.º 1950/17.0T9LSB-A.L1-5, de 06-02- 2018.

conteúdo do correio eletrónico, pelo que compete exclusivamente ao JIC tomar conhecimento, em primeiro lugar, do conteúdo das mensagens apreendidas, constituindo a sua violação numa nulidade expressa e absoluta, reconduzindo ao regime de proibição de prova.

Porém, será difícil de acreditar ser possível encaminhar as mensagens até ao conhecimento do JIC sem, pelo menos parcialmente, tomar conhecimento do seu conteúdo, e de que este conseguirá tomar efetivo conhecimento de todas elas, sendo o JIC quem verdadeiramente fará a seleção das mais pertinentes, não havendo qualquer garantia nesse primeiro conhecimento do JIC, "Não pode transformar-se o JIC num super investigador judicial a quem frequentemente se recorre para que faça novas pesquisas nas mensagens de correio eletrónico à luz dos desenvolvimentos da investigação." [100].

Segundo a opinião de Rita Castanheira Neves[101], de forma a contrariar a dificuldade prática que decorre do facto de o correio eletrónico ser geralmente apreendido em grande número, deverá exigir-se que, durante a diligência, se tenha sempre em atenção que, para que a mesma seja eficaz, devem seguir-se "critérios estritos de abrangência" e apreender apenas as mensagens de correio eletrónico que se afigurem "realmente determinantes para a prova".

Claro é que a produção de prova e a sua apreciação estão em constante mudança, pois o que num primeiro momento pode ser irrelevante, mais tarde poderá tornar-se numa prova decisiva. É o que acontece com as escutas telefónicas (art. 187.º e 188.º do CPP), quando o legislador permitiu que, até à acusação, o MP identifique e utilize quaisquer comunicações que até ao momento não tiverem sido consideradas relevantes pelo JIC. Desta forma, é inquestionável que deve haver intervenção do JIC, porém, na opinião de Rui Cardoso, esta intervenção não tem que de ser necessariamente prévia, sendo a posterior igualmente adequada à sua função garantística dos direitos fundamentais[102].

Tendo em conta a matéria exposta, afigura-se inquestionável a intervenção do JIC na apreensão de correio eletrónico, de forma a garantir a proteção dos direitos fundamentais dos cidadãos, uma vez que, não só o CPP determina reservas da prática de alguns atos materiais exclusivamente ao JIC (como é o caso das buscas em escritórios de advogados serem presididas pelo juiz, previsto no art. 177.º, n.º 3, CPP), como também o

[100] CARDOSO, 2021, p. 163.
[101] NEVES, 2011, p. 275.
[102] *Idem*, p. 165.

art. 179.º, n.º 3 do CPP determina que "o juiz que tiver autorizado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida.".

Deste modo, havendo despacho judicial que autorize a apreensão de correio eletrónico, bem como o JIC ter o primeiro a ter conhecimento do conteúdo das mensagens apreendidas, resulta numa dupla garantia dos direitos fundamentais, evitando uma violação extrema e desnecessária dos direitos à privacidade e de correspondência por outros órgãos estatais.

CONCLUSÃO

Sendo cada vez mais relevante a utilização, como meio de prova no processo penal, das mensagens de correio eletrónico e registos de natureza semelhante que são encontradas em sistemas informáticos, será matéria onde se requer, com particular importância, a proteção de direitos fundamentais.

Por regra, a pesquisa, o conhecimento do conteúdo e a apreensão de correio eletrónico exigem prévia intervenção do JIC. Tal intervenção prévia poderá ser dispensada em situações excecionais.

As especificidades da apreensão de dados informáticos em geral e de correio eletrónico em especial, bem como a dificuldade em determinar antecipadamente onde irão ser encontrados dados de correio eletrónico, a dificuldade em separar a pesquisa que vise obter dados de correio eletrónico das pesquisas que tenham outra finalidade, seriam passíveis de justificar que, neste caso, a intervenção fosse apenas posterior.

No entanto, pode concluir-se que, como decorre do regime previsto no art. 179.º do CPP, subsiste a exigência de despacho judicial prévio para a apreensão de correio eletrónico, sendo considerado uma reserva absoluta do JIC. E, para além do despacho judicial prévio, configura-se como necessário ser o JIC o primeiro a tomar conhecimento do conteúdo das mensagens. Por regra, trata-se do primeiro órgão constitucionalmente autorizado a ter acesso a este conteúdo, exercendo o controlo sobre direitos fundamentais. Contudo, o MP e os OPC's podem obter acesso, em primeira mão, ao conteúdo das mensagens de forma excecional, respeitando o disposto no art. 252.º, n.º 2 e 3, do CPP.

Por tudo o que foi exposto, podemos concluir que quando em causa está uma atuação restritiva no âmbito dos direitos fundamentais, a intervenção de um juiz é essencial para uma tutela efetiva desses direitos, mesmo nos casos de conflitos de direitos fundamentais, onde deve haver uma cedência parcial pela salvaguarda de outros direitos jusconstitucionalmente consagrados. Ao abrigo da CRP, o juiz goza de uma competência exclusiva e não delegável de garantia dos direitos fundamentais no âmbito do processo criminal, pelo que a sua dispensa é constitucionalmente admissível apenas em situações pontuais e definidas com exatidão, não resultando numa violação excessiva dos direitos e, assim, ser passível de se resolver os conflitos que possam existir.

BIBLIOGRAFIA

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição, Universidade Católica Editora, 2011.

ALVES, Manuel João; GONÇALVES, Fernando, *A Prova do Crime, Meios legais para a sua obtenção*, Edições Almedina, 2009.

ANDRADE, Manuel da Costa, "*Bruscamente no verão passado", a Reforma do Código de Processo Penal – Observações Críticas sobre uma Lei que Podia e Devia ter sido Diferente,* Coimbra Editora, 2009.

ANDRADE, Manuel da Costa, "*Comentário ao artigo 194º do Código Penal*", *Comentário Conimbricense do Código Penal*, Tomo I, 2ª Edição, Coimbra Editora, maio de 2012.

ANTUNES, Maria João, *Direito Processual Penal*, 3ª edição, Edições Almedina, agosto 2021.

ARNES, André, *Digital Forensics*, John Wiley & Sons, 2018.

BRAVO, Rogério, "*Da não equiparação do conceito de correio eletrónico ao conceito tradicional de correspondência por carta*", Revista Polícia e Justiça, 3ª série, N.º 7, Coimbra Editora, janeiro-junho de 2006.

CALVÃO, Filipa; GUERRA, Clara, *Fórum de Proteção de Dados, Em foco o novo quadro legal Europeu*, *Anotação*, Comissão Nacional de Proteção de Dados, n.º 1 de julho, 2015.

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital, *Constituição da República Portuguesa Anotada,* Volume I, Coimbra Editora, 2007.

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, Ano 39, n.º 153, janeiro-março 2018.

CARDOSO, Rui, *A Apreensão de Correio Eletrónico após o Acórdão do Tribunal Constitucional n.º 687/2021: do juiz das liberdades ao juiz purificador investigador?*, Revista Portuguesa de Direito Constitucional, n.º 1, 2021.

CASEY, Eoghan, *Handbook of Digital Forensics and Investigation*, Elsevier Academic Press, 2010.

CORREIA, João Conde, *Artigo 179.º - Apreensão de Correspondência - Comentário Judiciário do Código de Processo Penal, Tomo II*, Almedina, 2019.

CORREIA, João Conde, *Cibercriminalidade e Prova Digital – Jurisdição Penal e Processual Penal,* julho 2018, Centro de Estudos Judiciários - http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_Ciber_PDigital2018.pdf

CORREIA, João Conde, *Prova digital: as leis que temos e a lei que deveríamos ter*, Revista do Ministério Público, Ano 35, n.º 139, julho-setembro 2014.

DIAS, Jorge Figueiredo, *Direito Processual Penal,* 1ª edição, Coimbra Editora, 2004.

FIDALGO, Sónia, *A Recolha de Prova em Suporte Eletrónico — Em Particular, a Apreensão de Correio Eletrónico*, Revista JULGAR n.º 38, Almedina, maio-agosto 2019.

MATA-MOUROS, Maria de Fátima, *Juiz das Liberdades Desconstrução de um Mito do Processo Penal*, Almedina, 2011.

MESQUITA, Paulo Dá, "*Prolegómenos sobre prova eletrónica e interceção de telecomunicações no direito processual penal português – o Código e a Lei do*

Cibercrime", Processo Penal, Prova e Sistema Judiciário, Wolters Kluwer, Coimbra Editora, 1ª edição, 2010.

MILITÃO, Renato Lopes, *A Propósito da Prova Digital no Processo Penal*, 2012.

NEVES, António Castanheira, *Sumários de Processo Criminal* (ed. Policopiada), Coimbra, 1968.

NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas em processo penal - Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de Prova*, Coimbra Editora, 2011.

NUNES, Duarte Rodrigues, *Os meios de Obtenção de Prova previstos na Lei do Cibercrime*, GESTLEGAL, 2ª edição, novembro 2021.

PINHEIRO, Alexandre Sousa, FERNANDES, Mário João de Brito, *Comentário à IV Revisão Constitucional,* Lisboa: AAFDL Editora, 1999.

PRADO, Geraldo, *A Cadeia de Custódia da Prova no Processo Penal,* Marcial Pons, 2020.

RAMALHO, David; COIMBRA, José, *A declaração de invalidade da Diretiva 2006/24/CE*...

RAMOS, Armando Dias, *A Prova Digital em Processo Penal,* Chiado Editora, 1.º edição, 2014.

REALE, Miguel, *Filosofia do Direito*, 8ª Tiragem da 20.º reimpressão, Editora Saraiva, 2010.

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

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV – Da Prova – Eletrónico- Digital e da Criminalidade Informático-Digital*, 1ª Edição, Rei dos Livros, 2011.

ROXIN, Claus, *Derecho Procesal Penal*, tradução da 25.ª Edição Alemã *Strafverfahrensrecht* de Gabriela Córdoba e Daniel Pastor, Buenos Aires: Editores del Puerto, 2000.

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

SILVA, Germano Marques da, *Curso de Processo Penal* – Vol. I e II, Verbo Editora, 2010.

SILVA, Germano Marques da, *Direito Processual Penal Português*, 2ª edição, Universidade Católica Editora, 2017.

SILVA, Germano Marques da, *Produção e Valoração da Prova em Processo Penal*, Revista do CEJ, 1.º Semestre 2006, n.º 4.

SILVEIRA, Alexandra; FREITAS, Pedro Miguel, *Implicações da Declaração de Invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da EU: uma leitura jusfundamental,* Revista de Direito, Estado e Telecomunicações, Brasília, v.9, maio de 2017.

VALENTE, Manuel Monteiro Guedes, *Cadeia de Custódia da Prova,* 3ª edição, Edições Almedina, 2021.

VENÂNCIO, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, 1ª edição, Coimbra Editora, 2011.

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

VERDELHO, Pedro, *A obtenção de prova no ambiente digital,* Revista do Ministério Público, Ano 25, n.º 99, julho-setembro 2004.

VERDELHO, Pedro, *A reforma penal portuguesa e o Cibercrime*, Revista do Ministério Público, Ano 27, n.º 108, outubro-dezembro 2006.

VERDELHO, Pedro, *Apreensão de Correio Eletrónico em Processo Penal*, Revista do Ministério Público, Ano 25, n.º 100, outubro-dezembro 2004.

JURISPRUDÊNCIA CONSULTADA

Acórdão do Tribunal Constitucional n.º 687/2021, processo n.º 830/2021, de 22/09/2021, dos relatores, Juiz Conselheiro JOSÉ ANTÓNIO TELES PEREIRA e Juíza Conselheira MARIA JOSÉ RANGEL DE MESQUITA.

Acórdão do Tribunal Constitucional n.º 403/2015, processo n.º 773/15, de 17/09/2015, do relator, Juiz Conselheiro JOSÉ ANTÓNIO TELES PEREIRA.

Acórdão do Tribunal da Relação de Guimarães, processo n.º 735/10.0GAPTL-A.G1, de 29/03/2011, do relator, Juíza-Desembargadora MARIA JOSÉ NOGUEIRA.

Acórdão do Tribunal da Relação de Lisboa, processo n.º 5412/08.9TDLSB-A.L1-5, de 11/01/2011, do relator, Juiz-Desembargador RICARDO CARDOSO.

Acórdão do Tribunal da Relação de Lisboa, processo n.º 581/12.6PLSNT-A.L1-5, de 22/01/2013, do relator, Juíza-Desembargadora, ALDA TOMÉ CASIMIRO.

Acórdão do Tribunal da Relação de Lisboa, processo n.º 1950/17.0T9LSB-A.L1-5, de 06/02/2018, do relator, Juiz-Desembargador JOÃO CARROLA.

Acórdão do Tribunal da Relação de Lisboa, processo n.º 184/12.5TELSB-R.L1-3, de 27/01/2021, do relator, Juiz-Desembargador RUI TEIXEIRA.