Instituto Superior de Ciências Policiais e Segurança Interna

Jéssica Eva Alves Bento
Aspirante a Oficial de Polícia

Dissertação de Mestrado em Segurança Pública

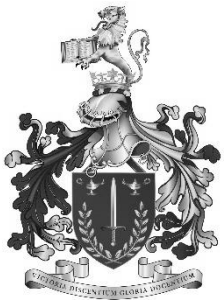
XXXVII Curso de Formação de Oficiais de Polícia

Da prova digital: A admissibilidade dos conhecimentos fortuitos no correio eletrónico

Orientadores:

Professor Doutor António Brito Neves
Subintendente Doutorando Carlos Correia

Lisboa, maio de 2025



Jéssica Eva Alves Bento

Aspirante a Oficial de Polícia

Dissertação de Mestrado em Segurança Pública

XXXVII Curso de Formação de Oficiais de Polícia

Da prova digital: A admissibilidade dos conhecimentos fortuitos no correio eletrónico

Dissertação apresentada no Instituto Superior de Ciências Policiais e Segurança Interna com vista à obtenção do grau de Mestre em Segurança Pública, elaborada sob a orientação do Professor Doutor António Brito Neves e do Subintendente Doutorando Carlos Correia.

Estabelecimento de Ensino:	Instituto Superior de Ciências Policiais e Segurança Interna
Curso:	XXXVII CFOP
Orientadores:	Professor Doutor António Brito Neves Subintendente Doutorando Carlos Correia
Título:	Da prova digital: A admissibilidade dos conhecimentos fortuitos no correio eletrónico
Autor:	Jéssica Eva Alves Bento
Local de Edição:	Lisboa
Data de Edição:	13 de maio de 2025

Dedicatória

Ao meu eu do futuro, que carregue com gratidão os ensinamentos do passado, honre o presente e lute com coragem para ser sempre uma versão melhor do que já foi!

Agradecimentos

Este é, sem dúvida, o momento que marca o encerramento de um ciclo de aprendizagens e crescimento, e o prenúncio de um novo começo. Nesta fase de especial nostalgia, agradeço em primeiro lugar a Deus, pela força e coragem que me acompanharam ao longo deste percurso.

Sou eternamente grata aos meus pais, espelho do amor mais puro que já conheci. Obrigada por serem o exemplo vivo de bondade, humanismo, honestidade e espírito de sacrifício. A vossa força, carácter e dedicação incondicional foram e serão sempre a minha inspiração diária.

Um agradecimento muito especial à minha saudosa avó Zulmira. Não há um só dia em que não me lembre de ti, com profunda saudade, ternura e amor. Obrigada por me ensinares o verdadeiro significado da vida - que me continues a guiar! Ao meu avô Zé, que sei que estaria orgulhoso por eu ter escolhido, como ele, servir o meu país.

A toda a minha família, que sempre me apoiou em todos os momentos, e a todos os meus amigos, que nunca me deixaram faltar motivação, compreensão e amor: o vosso apoio foi fundamental e uma constante fonte de inspiração.

Ao Gabriel e à sua família, obrigada por estes incansáveis anos de apoio, sempre presentes nos momentos mais determinantes.

Ao meu Orientador, Sr. Professor Doutor António Brito Neves, expresso o meu profundo agradecimento pelos valiosos contributos que tornaram possível a concretização de mais uma etapa.

Ao longo destes 5 anos, tive o privilégio de me inspirar em vários exemplos de excelência profissional, humanismo, dedicação e inteligência de vários profissionais que se cruzaram no meu caminho. Em especial, remeto a mais sincera gratidão, ao meu Coorientador, Sr. Subintendente Carlos Correia, sem o seu precioso contributo e apoio, nada disto seria possível.

Ingressei nesta profissão movida pela admiração a todos os profissionais que, dia após dia, se dedicam com empenho a servir o cidadão. A todos os que encontram, nas mais diversas circunstâncias da vida, motivação para continuar a dar o seu melhor por Portugal — Muito obrigada!

Aquele que tem um porquê para viver, consegue suportar quase qualquer como!

Friedrich Nietzsche

Resumo

A tecnologia está presente em todos os aspetos das sociedades atuais, influenciando desde os novos métodos de cibercriminalidade aos mais recentes procedimentos de investigação criminal e métodos processuais penais. Neste contexto, a prova digital adquire uma centralidade cada vez maior nos processos da atualidade, embora apresente uma natureza instável, volátil e a sua investigação mereça particular atenção, tendo em conta a sua relevância jurídica. A crescente utilização das mensagens do correio eletrónico, enquanto meio de prova no processo penal, tornou evidente a necessidade de um enquadramento e um regime jurídico que atenda à natureza deste meio de prova. Neste âmbito, a presente dissertação concentrou-se numa análise doutrinária e jurisprudencial do art.º 17.º da Lei do Cibercrime, sobre o regime da apreensão de correio eletrónico e registos de comunicações de natureza semelhante. A força motriz deste estudo dedicou-se a compreender a admissibilidade dos conhecimentos fortuitos no correio eletrónico, distinguindo-os de conhecimentos de investigação e de *phishing expeditions.* Este estudo trouxe discussões doutrinárias e várias perspetivas jurisprudenciais sobre problemáticas associadas à coexistência de vários regimes processuais de âmbito do regime da apreensão do correio eletrónico. Face à omissão legal, a análise permitiu concluir que, na prática, tem sido sustentado que os conhecimentos fortuitos provenientes da apreensão de correio eletrónico, podem ser admissíveis e usados num processo distinto, desde que sejam respeitados os princípios da legalidade, da necessidade, da proporcionalidade, da reserva de juiz e sempre que se garanta o cumprimento rigoroso dos requisitos da apreensão fruto da investigação original. Este processo deve respeitar uma análise casuística rigorosa, sempre sujeita a controlo judicial.

Palavras-chave: cibercriminalidade; conhecimentos fortuitos; correio eletrónico; Lei do Cibercrime; prova digital.

Abstract

Technology is present in every aspect of today's societies, influencing everything from new cybercrime methods to the latest criminal investigation procedures and criminal procedure methods. In this context, digital evidence is increasingly central to today's processes, although it is unstable and volatile and its investigation deserves particular attention, given its legal relevance. The growing use of e-mails as evidence in criminal proceedings has made it clear that there is a need for a framework and a legal regime that takes into account the nature of this evidence. In this context, this dissertation focused on a doctrinal and jurisprudential analysis of article 17 of the Cybercrime Law, on the regime for seizing emails and records of communications of a similar nature. The driving force behind this study was to understand the admissibility of fortuitous knowledge in electronic mail, distinguishing it from investigative knowledge and phishing expeditions. This study brought together doctrinal discussions and various jurisprudential perspectives on the problems associated with the coexistence of various procedural regimes for the seizure of electronic mail. Despite the legal omission, the results have shown that fortuitous knowledge from the seizure of emails can be admissible and used in a separate case, provided that the principles of legality, necessity, proportionality and the reserve of the judge are respected, and provided that strict compliance with the requirements of the seizure resulting from the original investigation is guaranteed.

Keywords: cybercrime; fortuitous knowledge; electronic mail; Cybercrime Law; digital evidence.

Lista de Siglas, Acrónimos e Abreviaturas

Ac.	Acórdão
AJ	Autoridade Judiciária
al.	Alínea
APC	Autoridade de Polícia Criminal
art.º(s)	Artigo(s)
CC	Código Civil
CCiber	Convenção sobre o Cibercrime
Cf.	Conforme
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
EUA	Estados Unidos da América
GPS	*Global Position System*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
JIC	Juiz de Instrução Criminal
LCC	Lei do Cibercrime
LSI	Lei de Segurança Interna
MP	Ministério Público
OPC(s)	Órgão(s) de Polícia Criminal
p./pp.	Página(s)
PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública

STJ	Supremo Tribunal de Justiça
TC	Tribunal Constitucional
TEDH	Tribunal Europeu dos Direitos Humanos
TGR	Tribunal da Relação de Guimarães
TRE	Tribunal da Relação de Évora
TRL	Tribunal da Relação de Lisboa
TRP	Tribunal da Relação do Porto

Índice

Introdução

A era digital contemplou-nos com um "gigantesco repositório de informações acessíveis" (Contardo, 2020, p. 279) porém, também gerou uma dependência tecnológica profunda e irreversível, que hoje se manifesta em "todas as ciências e todas as realidades, afetando, em particular a vida social e humana" (Meireles, 2023, pp. 92-93). Como parte integrante deste fenómeno, emerge a sociedade digital (Valente, 2019).

O ciberespaço veio revolucionar vários aspetos sociais, desde as interações humanas à noção de privacidade e, para combater as novas ameaças provenientes do ambiente digital, foi necessária uma adaptação transformadora das normas jurídicas que ainda se mantêm em transição. Assim, no contexto jurídico, tem-se observado um processo de desmaterialização de documentos, com a sua disponibilização em plataformas digitais. Do mesmo modo, também determinados procedimentos legais, como a audição de testemunhas, passaram a ser realizadas através de videoconferência eletrónica (Mendes, 2021).

Em síntese, podemos afirmar que a transformação digital influencia todos os aspetos da vida em sociedade, refletindo-se também no fenómeno criminal e na administração da justiça, sendo "a tecnologia (…) uma espécie de amplificador aplicado às nossas naturezas" (Meireles, 2023, p. 94). Com efeito, estes avanços tecnológicos permitiram o emergir de novos conceitos como a cibercriminalidade, e tudo isto nos conduziu à sociedade da informação e da comunicação (Clemente, 2021).

Tanto no Direito Penal como no Direito Processual Penal, a prova digital tem sido objeto de investigação, enquanto meio de obtenção de prova ou meio de prova *per se.* Todas estas alterações permitiram a criação de um novo padrão de atuação da investigação criminal.

Cabe salientar que, a complexidade legal inerente à apreensão do correio eletrónico, permitiu a criação de normas que se sobrepõem às que já existiam, onde produzem uma zona de atuação cinzenta em que a coexistência das Leis, se reflete na complexidade da sua aplicação prática.

Perante isto, e no que à prova digital diz respeito, cabe ao legislador criar soluções normativas claras e eficientes, que acompanhem os avanços tecnológicos da era digital.

Já defendia Correia (2014) que,

> a qualidade da Lei vigente é condição essencial para a qualidade do direito quotidianamente aplicado: sem uma boa Lei, por melhores que sejam os nossos juristas, dificilmente haverá bom direito. Por outro lado, porque o constante progresso científico reclama uma atuação constante do legislador. É necessário que ele adeque o direito processual penal às novas realidades disponibilizadas pelo contínuo progresso científico e logo utilizadas pela criminalidade (Correia, 2014, p. 53).

Duas observações. A primeira, para referir que, no decorrer deste estudo, iremos salientar a missão atribuída à PSP, prevista na Lei n.º 53/2007, de 31 de agosto, que a define, destacando entre outras, o seu compromisso em garantir a legalidade democrática, a segurança interna, os direitos dos cidadãos, assegurar a ordem e a tranquilidade pública e prevenir a criminalidade. A segunda, para salientar que, de acordo com estas diretrizes, a PSP é responsável pelas ações de investigação criminal, que obedecem ao disposto na Lei n.º 49/2008, de 27 de agosto, que outorga a Lei de Organização da Investigação Criminal.

Nesta senda, a Investigação Criminal desenvolvida pela PSP, tem tido o dever de enfrentar desafios cada vez mais complexos. Como refere Correia (2014) "A prova digital, (…) atualmente constitui o cerne da generalidade dos nossos processos penais" (p. 1), e delimita o objeto da presente dissertação, pertencendo-a num universo abrangente e fundamental para as atividades de investigação criminal da PSP.

Ao longo deste estudo, iremos detalhar o conceito de prova digital, autonomizando-a do correio eletrónico como meio de prova digital. Assim, serão analisadas questões relevantes quanto à sua apreensão, bem como a admissibilidade dos conhecimentos fortuitos no correio eletrónico.

Delimitando o objeto da dissertação, a problemática deste estudo centra-se no facto de não existir uma previsão legal específica expressa, que justifique a admissibilidade de conhecimentos fortuitos no âmbito da apreensão do correio eletrónico. No entanto, o art.º 187.º, números 7 e 8, do CPP valida nos casos expressos, a valoração como prova dos conhecimentos fortuitos, no regime das escutas telefónicas.

Desta forma, cumpre indicar a sequência da exposição para orientação do leitor, em primeiro lugar, procuraremos definir conceitos relevantes no âmbito da prova digital,

identificando o seu regime jurídico. Neste sentido, abordaremos detalhadamente os diferentes regimes legais aplicáveis à apreensão de correio eletrónico e registos de comunicações de natureza semelhante, e exploraremos os ditames da sua concretização prática, mediante um paralelismo com base na Lei n.º 109/2009, de 15 de setembro, o regime das escutas telefónicas, o regime geral das apreensões e o regime da apreensão da correspondência, entre outros normativos legais que se vislumbrem relevantes.

De seguida, cabe proceder à distinção entre o correio eletrónico fechado e não lido, do aberto e lido, de acordo com a doutrina, para determinar o regime adequado a cada caso (Cf. ocorre no regime da apreensão de correspondência, previsto no CPP nos art.º(s) 179.º e 252.º). Analisaremos as várias medidas de admissibilidade da apreensão do correio eletrónico em processos distintos daqueles que remetem para os conhecimentos da investigação que lhe deu origem.

Esta dissertação estrutura-se em quatro capítulos e incluirá uma abordagem aos desafios práticos enfrentados pela Investigação Criminal da PSP, na obtenção e na utilização da prova digital, onde se inclui, a recolha de metadados, a identificação de endereços IP, e a recolha de cabeçalhos do correio eletrónico para atestar a veracidade do *email*.

Em suma, trata-se de um tema com relevância teórico-prática, pelo que esperamos dar o nosso modesto contributo na investigação, com especial ênfase na importância de um equilíbrio entre a eficácia probatória e a proteção dos direitos fundamentais, no âmbito da admissibilidade da prova digital face à afetação da privacidade e dos demais direitos dos cidadãos, que se vêm restringidos no caso da apreensão do correio eletrónico.

Deste modo, espera-se que esta dissertação contribua para a compreensão dos desafios inerentes à admissibilidade dos conhecimentos fortuitos no correio eletrónico e para a construção de debates que pensem soluções de um equilíbrio entre a eficácia da investigação criminal e a proteção dos direitos, liberdades e garantias dos cidadãos.

Problema de Investigação

A presente dissertação parte da crescente digitalização da sociedade e da evolução tecnológica para apresentar alguns desafios importantes para a investigação criminal da PSP, essencialmente nos desafios inerentes à obtenção da prova digital e à sua admissibilidade. A apreensão do correio eletrónico tem tido frequentemente importância ao nível das investigações, contudo, tem levantado questões complexas relativas à proteção dos direitos fundamentais e aos limites legais da sua utilização como meio de prova.

Neste cenário, a vastidão do espaço digital e a diversidade de conteúdos e informações acessíveis durante a apreensão do correio eletrónico, colocam novos desafios à investigação criminal da PSP. Entre eles, destacam-se os conhecimentos fortuitos, cuja apreensão e admissibilidade como meio de prova se revela particularmente complexa.

Deste modo, a presente dissertação propõe-se responder à seguinte questão central: Em que casos, no ordenamento jurídico português, os conhecimentos fortuitos obtidos no correio eletrónico podem ser considerados admissíveis como meio de prova na investigação criminal?

Método

Para responder à questão anterior, neste trabalho científico utilizámos a revisão da literatura com base no método dedutivo, e a interpretação da doutrina e do direito, amplamente requerido para analisar questões da natureza jurídica. O estudo foi desenvolvido através de uma pesquisa bibliográfica, recorrendo à legislação nacional e a diversos acórdãos, bem como a doutrina relevante, tanto a nível nacional como internacional.

A estrutura da investigação inicia-se com um enquadramento geral sobre a prova no processo penal e a evolução da prova digital, abordando os desafios inerentes à sua recolha e admissibilidade. Em seguida, será analisado o regime jurídico da prova digital em Portugal, com especial atenção ao correio eletrónico como meio de prova, incluindo os limites à sua apreensão e o impacto na tutela dos direitos fundamentais. Nesta fase, transportaremos o leitor para uma abordagem prática dos desafios intrínsecos à atividade da investigação criminal da PSP na apreensão desta prova. No quarto capítulo, será aprofundada a temática dos conhecimentos fortuitos, diferenciando-os de outras figuras como, os conhecimentos de investigação e as chamadas *phishing expeditions*. Por fim dedicaremos especial atenção à admissibilidade dos conhecimentos fortuitos no correio eletrónico, como foco do presente estudo.

Capítulo I. O enquadramento geral da prova no processo penal e a prova digital

1.1 A relevância da prova no processo penal

A prova tem uma importância indiscutível no processo penal, admitindo o poder de transportar o julgador a uma realidade alegada que não presenciou, nem conhece (Meireles, 2023).

As provas servem manifestamente para a reconstituição da realidade, uma vez que, no momento da sentença declarada pelo juiz, essa realidade já não existe (Ruço, 2017).

Nestes moldes, é a prova que permite ao julgador compreender amplamente o cenário criminal, conhecendo os factos e posteriormente decidir a seu respeito, aplicando o direito adequado ao caso concreto, de acordo com a máxima "*narra mihi factum, dabo tibi ius* (narra-me os factos, e dar-te-ei o Direito)" (Brandão, 2019, p. 19).

Trata-se de uma forma de demonstrar a realidade dos factos, essencial para a realização da justiça, à luz do art.º 341.º do CC, subsidiariamente aplicável ao processo penal, sempre que não seja contrariada pelos princípios de direito penal e processual penal, sendo complementada pelos princípios descritos nos art.º(s) 125.º (legalidade da prova) e 127.º (livre apreciação da prova) do CPP (Brandão, 2019).

Em processo penal, a obtenção da prova tem o objetivo de determinar se os factos qualificados como crimes, foram praticados, determinar quem os praticou e sob que circunstâncias, reunindo os elementos de prova necessários para o apuramento da verdade. Todos estes elementos probatórios são essenciais para serem reunidos em sede de tribunal e permitir que os culpados sejam condenados. No entanto, este processo ocorre, sempre respeitando os direitos fundamentais que cabem aos visados e todas as garantias que a Lei lhes confere neste âmbito (Verdelho, 2004).

Determinam os art.º(s) 125.º e 127.º do CPP, que são permitidas as provas que não forem proibidas por Lei e que cada elemento de prova é dissecado com base na experiência e livre convicção do julgador. Contudo, o juízo técnico, científico ou artístico intrínseco à prova pericial, encontra-se subtraído à livre apreciação do julgador, de acordo com o art.º 163.º do CPP. Verdelho (2004) sustenta que a prova pericial está sujeita a uma especial autoridade técnica no CPP, pela sua natureza científica.

O Ac. do Tribunal da Relação de Coimbra, de 11/12/2024 defende que por mais que se diga que o juiz é o perito dos peritos, na grande maioria dos casos, o laudo pericial desempenha um papel fundamental na decisão da causa. O juiz não tem uma liberdade total na apreciação da prova, uma vez que recorre a critérios racionais fundamentados, deste modo, a prova pericial não tem uma presunção *juris et jure* face ao princípio da livre convicção do julgador (Verdelho, 2004).

Pode-se afirmar que cabe ao investigador o exercício rigoroso, diligente e estratégico inerente à sua função, de utilizar os meios ao seu dispor para a descoberta da verdade, respeitando os limites legais e as garantias constitucionais (Verdelho, 2004).

1.2. Limites jurídicos para a obtenção da prova

Na sociedade atual, dominada pelas tecnologias de informação e comunicação, a liberdade de expressão, entre outras garantias fundamentais, assume uma complexidade acrescida, exigindo uma análise cuidada para a clarificação das fronteiras entre direitos individuais e a realização da justiça. A progressiva digitalização, não só influencia a forma como a informação é armazenada, mas também levanta questões sobre a proteção jurídica das comunicações eletrónicas. As liberdades individuais adquirem um espaço complexo em contraste com outros direitos ou com a prossecução da justiça. "Quer na Europa, quer nos EUA, a emergência da sociedade da informação tornou manifesta uma tendência no sentido da ampliação e reforço da proteção jurídica das formas de criação e tratamento da informação tornadas possíveis pelo sistema computador/telecomunicações." (Gonçalves, 2024, p. 67)

No contexto da prova digital, a obtenção de elementos probatórios deve ser acuradamente ponderada, evitando que a justiça se sobreponha indevidamente à proteção dos direitos fundamentais. A descoberta da verdade, não pode por si só, ser motivo suficiente para a efetivação da justiça através de provas obtidas mediante ofensas à integridade física ou moral das pessoas, coação, abusiva intromissão na vida privada, no domicílio ou nas telecomunicações. Estes meios ofensivos estão expressos no n.º 8 do art.º 32.º da CRP, devidamente inseridos enquanto uma das principais garantias do processo criminal (Andrade, 1992).

O art.º 32.º da CRP estabelece o princípio das proibições de prova, articulando-se com o art.º 122.º do CPP que prevê que as nulidades têm impactos de invalidade nos atos em que se verificarem e sob os quais dependerem e puderem afetar. Este regime é

complementado pelo art.º 126.º do CPP, que proíbe a utilização de todas as provas obtidas mediante métodos proibidos (Andrade, 1992).

Desde 1987[1] que o art.º 126.º do CPP foi a concretização constitucional dos métodos proibidos de prova, o n.º 1 do mesmo artigo, condensa as proibições absolutas, que constam em parte na redação do n.º 2, onde o consentimento do visado é insuscetível de servir para a validação das provas com base nos métodos descritos. O n.º 3 do mesmo artigo, apresenta as proibições relativas de provas, obtidas com intromissão na privacidade, cuja admissibilidade depende do expresso consentimento do titular dos direitos afetados, ou em determinados casos em que a intromissão respeite os termos legais. Com isto, pretendemos fazer referência aos casos em que sejam autorizados por lei, a prova seja sujeita a um controlo judicial, a existência de fundamentação legal que justifique essa intromissão e o respeito pelos princípios constitucionais (Ramalho, 2017).

Embora as proibições de prova estabeleçam limites substanciais à obtenção de elementos probatórios no processo penal, as regras de produção de prova desempenham um papel distinto. Enquanto as proibições de prova delimitam as fronteiras legais da atividade probatória, as regras de produção de prova visam assegurar a conformidade legal dos meios utilizados na obtenção de provas (Andrade, 1992).

Assim, as proibições de prova impõem uma fronteira legal, ao passo que as regras de produção de prova garantem a legalidade e o respeito pelos direitos fundamentais durante o processo probatório (Andrade, 1992).

Para Dias (2004) as regras de produção de prova são essenciais, atendendo à qualidade dos bens jurídicos em causa, e constituem-se como uma forma de impedir sacrifícios desnecessários e desproporcionais, garantindo um equilíbrio vital ao processo e à justiça.

As proibições de prova carecem de uma análise ao caso concreto, através da ponderação da necessidade, dos interesses em causa e da proporcionalidade entre os bens jurídicos que são sacrificados e os que são invocados. Em diversos casos, o recurso a determinados meios de prova proibidos é assegurado com base no direito de necessidade, ou a legítima defesa, quando esteja em causa a "promoção de interesses transcendentes ao processo penal". Contudo, ao estarem em causa direitos fundamentais, estes não representam uma justificação para uma prática ilegal, mas para no extremo se ponderar

[1] Foi em 1987 que se deu a materialização da responsabilidade do legislador consagrar no plano inconstitucional os limites legais e éticos das provas.

se o sacrifício de um direito pode ser compensado pela proteção de outro de maior valor (Andrade, 1992, p. 83).

Porém, a imposição dos interesses do Estado não pode significar a submissão e conversão do cidadão a um mero objeto "fonte de informações", abdicando da sua dignidade (Hassemer, 1990, p. 202).

1.3. Meios de prova e meios de obtenção de prova

Primeiramente importa estabelecer uma distinção clara entre os meios de obtenção de prova e os meios de prova *per se.* Estes últimos encontram-se definidos a partir do art.º 128.º do CPP, até ao art.º 170.º do mesmo diploma, contando com a prova testemunhal (art.º 128.º, e 129.º do CPP), as declarações do arguido (art.º 140.º e 141.º do CPP), a prova por acareação (art.º 146.º do CPP), a prova por reconhecimento (art.º 147.º do CPP), a prova por reconstituição (art.º 150.º do CPP), a prova pericial (art.º 151.º do CPP) e a prova documental (art.º 164.º do CPP) (Almeida, 2018).

Silva (2008) refere que os meios de obtenção de prova são instrumentos que auxiliam o investigador e as autoridades judiciárias a recolher os meios de prova do processo em curso, diferenciando-se dos meios de prova pela sua "perspetiva lógica e técnico-operativa" (p. 233). A perspetiva lógica diz respeito à avaliação da prova com base na coerência dos factos e evidências, que têm a capacidade de permitir formular juízos de valor sobre a culpabilidade do arguido. Enquanto que, a perspetiva técnico-operativa diz respeito a questões sobre a legalidade dos meios de obtenção de prova e a admissibilidade das mesmas, nomeadamente no inquérito, consoante os limites estabelecidos para a aquisição da prova na investigação (Silva, 2008).

Segundo Andrade (1992) existe uma sistematização no CPP dos meios de obtenção de prova, (exames, revistas e buscas, apreensões e escutas telefónicas), que aparecem elencados por esta ordem, gradualmente, de acordo com a intensidade da restrição dos direitos fundamentais.

Os meios de obtenção de prova correspondem aos métodos utilizados para aceder aos elementos de prova necessários que formam a convicção do julgador (Brandão, 2019).

Valente (2004), argumenta que existe uma transição sistemática hierarquizada dos meios de obtenção de prova, para aferir a

> probabilidade de ferimento de direitos fundamentais – integridade pessoal, reserva da intimidade da vida privada, inviolabilidade do domicílio e das telecomunicações e da correspondência, imagem, palavra, honra – como se existisse uma escada ascendente a subir de acordo com o esgotamento da anterior e da necessidade para defesa da coletividade e do próprio agente ou suspeito do crime com fins de prevenção geral e especial (pp. 50-51)

Contudo, o ordenamento jurídico português não consagra formalmente uma hierarquia que só permita o uso de um método de obtenção de prova se o anterior se esgotar. O CPP estabelece um regime ancorado nos princípios da legalidade, da necessidade e da proporcionalidade (Cf. art.º(s) 125.º e 126.º do CPP), e cada meio deve ser avaliado casuisticamente. O art.º 18.º, n.º 2 da CRP refere expressamente que os direitos fundamentais só podem ser restringidos na medida do necessário, devendo os meios de obtenção de prova ser antes escolhidos com base num juízo de necessidade, proporcionalidade e adequação ao caso em concreto.

1.4. O surgimento da prova digital

Há algumas décadas, seria inimaginável que os elementos essenciais para a investigação de crimes fossem encontrados predominantemente em ambiente digital. Na atualidade, a prova digital tornou-se indispensável, devido à sua ampla capacidade de fornecer material probatório relevante, para apurar a veracidade dos factos (Almeida, 2018).

O avanço tecnológico condensado nas últimas décadas foi suficiente para atualmente assistirmos à supremacia das tecnologias, e vermos a nossa vida "dominada pela informática e pela eletrónica" (Monteiro, 2023, p. 552).

Para acompanhar o desenvolvimento, e combater o recente tipo de criminalidade, surgiram novas técnicas de investigação, novas especializações, novos métodos de obtenção de prova, e a prova em suporte eletrónico (Hermeiro, 2023).

Na investigação criminal contemporânea, face à elevada complexidade do *modus operandi* da criminalidade, a prova pericial, prevista no art.º 151.º do CPP, configura um dos instrumentos de maior relevância e destaque, exigindo um rigor analítico que a coloca no cerne da procura pela verdade material (Verdelho, 2004).

A ciência forense digital orienta a investigação criminal em termos de "criminalidade informático-digital, para a preservação, recolha, gravação, validação, identificação, análise, interpretação, documentação e apresentação deste específico tipo de prova" (Rodrigues, 2009, p. 569).

Ramalho (2017) define que o ambiente digital engloba o que diz respeito aos dados informáticos que são desenvolvidos e processados em sistemas informáticos, onde podem ser diretamente ou virtualmente acedidos.

A obtenção de provas em ambiente digital caracteriza-se por uma potencialidade de horizontes ilimitados, oferecendo um campo de pesquisa com possibilidades praticamente inesgotáveis de conteúdo e informações. As perícias facilitam sobretudo a nível digital, na descoberta e apuramento dos factos, bem como na produção da prova. Quando a complexidade do caso não justifica a necessidade de realização de uma perícia, é possível recorrer aos exames previstos no art.º 354.º do CPP (Verdelho, 2004).

1.5. Prova digital, o conceito e a sua relevância

Por opção do legislador, não existe delimitação legal do conceito de prova digital, cabe então tanto à doutrina como à jurisprudência, alcançar definições para esta prova. Nunes (2021) opta por defender que a prova digital é toda a

> informação relevante para fins probatórios produzida/obtida a partir de dados em formato digital (na forma binária, em que todas as quantidades se representam pelos números 0 ou 1) armazenados, processados ou transmitidos em /através de/entre sistemas informáticos ou armazenados em suportes informáticos, muitas vezes com utilização de redes de comunicações eletrónicas (Nunes, 2021, p. 47).

Para concretizar o conceito de prova digital, Rodrigues (2009) define o termo como "prova eletrónico-digital" (p. 573), como informação de valor probatório, que pode ser armazenada ou transmitida sob a forma binária ou digital. A informação recolhida é examinada e este processo deve estar em concordância com as regras da produção de prova.

Sustentando uma opinião distinta, Ramalho (2017) esclarece que a prova digital e a prova eletrónica diferem uma da outra, e apresentam características especificas face à prova física. Esta particularidade torna evidente a desconformidade da aplicação das normas processuais tradicionais na prova digital.

Monteiro (2023) também afirma que a prova eletrónica difere da prova digital, uma vez que considera que na primeira definição cabem mais tipos de prova, pois engloba tanto a prova obtida mediante dados digitais, como a partir de formato analógico. Defende ainda que, todos os documentos digitais são documentos eletrónicos, porém o inverso não se aplica.

O mesmo autor esclarece que a prova digital pode ser fornecida por dispositivos tecnológicos em uso frequente na atualidade, tais como o computador, telemóvel, *smartwatches,* sistemas de localização GPS, e dispositivos fotográficos. Os dados essenciais para servir de prova, recolhidos a partir destes dispositivos, como os *email*s, mensagens, imagens, são uma prova de grande importância, pois são desde logo, fruto da dependência tecnológica da atualidade e, como tal usados frequentemente (Monteiro, 2023).

Almeida (2018) reconhece que é fundamental que os factos retenham valor probatório suficiente para criar convicção no julgador sobre a autenticidade dos mesmos, mas também que seja possível conservar a prova que, neste caso tem o formato digital Este autor reconhece que a prova digital oferece uma oportunidade imensurável de conteúdos probatórios e ao mesmo tempo detém a capacidade de lhes aceder de forma remota e célere.

Na definição de Fidalgo (2022) a prova digital é produzida por dados em "formato digital na forma binária, que são manipulados, armazenados ou comunicados através de qualquer dispositivo, computador ou sistema informático, ou transmitidos através de um sistema de comunicação" (p. 133).

No entanto, para Ramos (2014) a prova digital é

> toda a informação passível de ser obtida ou 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 também ser autêntica, precisa e completa (p. 77).

A recolha desta prova é fundamental para qualquer tipologia criminal, e não se restringe apenas a crimes informáticos. Esta é uma prova documental que, de acordo com o art.º 362.º do CC é um "documento ou qualquer objeto elaborado pelo homem com o fim de reproduzir ou representar uma pessoa, coisa ou facto" (Nunes, 2021, p. 47). No mesmo sentido, também Ramos (2014) salienta que a prova digital pode ser classificada como prova documental sempre que possa ser "corporizada em escrito ou por outro meio técnico, como, por exemplo, a impressão fotográfica ou audiovisual de uma mensagem de correio eletrónico" (p. 78).

De acordo com a lógica delineada por Ramos (2014), a prova digital pode assumir a natureza da prova pericial (Cf. art.º(s) 151º, 152º e 153º), na medida em que, a sua análise, apreciação e interpretação requerem conhecimentos técnicos, científicos ou artísticos especializados para apurar os factos.

Contudo, persiste uma ausência de definição precisa ou consenso relativamente ao conceito de prova digital, que permanece em constante evolução (Monteiro, 2023).

Almeida (2018) faz ainda a importante distinção entre prova digital enquanto meio de prova que, atesta a veracidade dos factos e comprova alegações fundamentais para construir a convicção do julgador face ao dolo, mas também enquanto meio de obtenção de prova, capaz de ser o cerne de determinadas investigações, sendo que não se limita apenas à cibercriminalidade. É um meio de obtenção de prova célere que, apesar de não ser um meio tradicional, como os restantes representados no CPP, é na atualidade basilar para as investigações. A prova digital permite

> a localização, identificação, e delimitação dos infratores no que concerne a crimes que pela sua natureza tecnológica, seria impossível ou muito complicado, extrair uma prova sustentada, capaz de criar convicção, de todo o modo operacional praticado pelos executantes (*modus operandi*) do crime ou ilícito. (Almeida, 2018, p. 35).

Importa esclarecer que este estudo centrar-se-á especificamente numa análise da mensagem de correio eletrónico, restringindo-se, por conseguinte, ao regime jurídico aplicável à sua apreensão e utilização como meio de prova. Embora existam outros meios de prova digital, que não serão objeto de exploração designadamente, a prova documental, visual ou sonora, produzida pelo Skype; a prova documental, visual ou sonora, produzida pelas redes sociais; as plataformas digitais; o *whatsapp*; a fotografia digital; gravações de

vídeo e de áudio; o ficheiro informático; o *printscreen* e a assinatura digital (Meireles, 2023). O regime jurídico destas provas pode apresentar particularidades distintas, razão pela qual não serão objeto de análise na presente dissertação.

1.6. Os desafios e as características da natureza da prova digital

Devido à natureza volátil da prova digital, na sua relação com o espaço onde pode ser encontrada, uma vez que acedemos à internet em vários locais e através de vários meios tecnológicos, é difícil determinar com exatidão, o local onde foi efetivada a prática criminal e o momento em que o infrator cometeu o crime (Almeida, 2018).

Em primeiro lugar, a prova digital pode encontrar-se armazenada em diversos suportes informáticos, desde telemóveis, computadores, *tablets*, discos externos… Por outro lado, esta prova pode estar na posse de pessoas que não estão diretamente ligadas à prática do crime. A prova digital não revela, em regra, uma relação previsível nem facilmente detetável entre o autor e o objeto do ilícito criminal. No momento da investigação, a apreensão da prova deve ser realizada com o máximo de rigor possível, atendendo à facilidade com que qualquer indício pode ser perdido, com algo tão simples como um toque numa tecla que pode apagar alguma informação fundamental, ou o histórico de navegação. Devido à possibilidade de edição da hora em que determinado facto ocorre, é de extrema complexidade para o investigador chegar ao momento exato em que o agente praticou o crime (Almeida, 2018).

No mesmo sentido, argumentava Rodrigues (2014) relativamente à efemeridade, instabilidade e fragilidade desta prova, cujas características podem colocar em causa o seu valor probatório.

Esta prova apresenta desde logo dificuldade quanto aos procedimentos a adotar na investigação e na recolha, atendendo a que é o cerne do método probatório, estes procedimentos vão condicionar o resultado da investigação e, consequentemente do processo (Hermeiro, 2023).

Esta prova merece ser tratada de acordo com a sua especificidade, dada a facilidade em torná-la inutilizável, o que condiciona diretamente a força probatória, a admissibilidade da prova em tribunal, e cria dúvidas relativamente à fiabilidade da prova (Rodrigues, 2009).

No âmbito do trabalho de um jurista, o tratamento de uma prova tradicional não se dá da mesma forma da prova digital, que carece de competências especificas ao nível

da informática, nomeadamente da capacidade de operar em *cloud computing*, justamente porque este mecanismo utiliza a memória virtual e a capacidade de armazenamento online da informação e dados, entre vários servidores interligados pela internet. Este servidor pode ser acedido em qualquer localização e momento, remotamente ou através da internet (Almeida, 2018).

> Todo e qualquer dispositivo, independentemente do local onde se encontra, pode aceder a uma rede, pública ou privada, e desde aí, operar na mais vasta panóplia de ações, como consulta, acesso a dados, cópia destes, alteração (…) acesso a pacotes de dados de terceiros, podendo tantas vezes, usá-los como seus, e/ou, beneficiando ou prejudicando outrem, com esse acesso privilegiado (Almeida, 2018, p. 44).

No mesmo sentido, Ramos (2014) reforça a ideia de que os conhecimentos técnicos não são por si só suficientes, durante a investigação, mas também se requer ao investigador competências especificas para o processo de apreensão, manuseamento ou transporte, tal como os procedimentos de análise ou exame, aquando da apreensão da prova digital.

Nesta senda, no contexto específico da atuação da PSP, sustento que deve ser necessária uma formação especializada que garanta não só a integridade da prova, como o respeito pelos princípios constitucionais e a autenticidade da cadeia de custódia. Para além de uma competência técnica ao nível da recolha da prova em suporte eletrónico, devem ser sempre dotados da formação jurídica necessária para garantir o respeito pelos direitos fundamentais e o cumprimento dos requisitos legais para a admissibilidade da prova.

Relativamente à autenticidade da prova digital, em determinadas situações é uma prova onde a sua fiabilidade é questionada, dado que é difícil identificar o agente que acedeu à rede e praticou os factos e qualquer código de identificação ou de rede é suscetível de ser manipulado. Esta identificação ocorre a partir do endereço IP, pois cada dispositivo eletrónico tem um número único que permite a comunicação em rede com os demais dispositivos e sistemas, este IP apenas transmite dados relativos à localização e informação do mesmo (Almeida, 2018).

Almeida (2018) refere que a única forma de se asseverar com alguma fiabilidade (sempre admitindo a possibilidade de erros) a identificação de alguém nestes termos, é através do uso da assinatura eletrónica em documentos, como forma de autenticação.

O mesmo autor compara a assinatura eletrónica a um *login* efetuado através da inserção de credenciais de um utilizador numa plataforma digital mediante uma palavra-passe individual que lhe permite aceder a uma área pessoal. Ainda assim, um terceiro pode ter acesso a estes dados e isso vai inviabilizar a probabilidade de se afirmar que quem acedeu naquele momento com aquelas credenciais foi determinada pessoa. Com isto, os indícios não são suficientes para se responsabilizar um arguido (Almeida, 2018).

No que toca à sua admissibilidade, todas as provas são admitidas desde que, os procedimentos e critérios para a sua obtenção tenham sido respeitados e regidos pelos princípios da legalidade e objetividade, pois caso isso não ocorra, estaríamos perante a *fruits of the poisonous tree doctrine*[2](Andrade, 1992; Rodrigues, 2014).

Relativamente ao percurso que esta prova enfrenta desde a sua recolha, análise, armazenamento, preservação até à sua valoração, importa referir que a cadeia de custódia da prova digital constitui um processo altamente completo, exigindo deste modo, um esforço acrescido na manutenção da integridade, fiabilidade e autenticidade (Hermeiro, 2023; Rodrigues, 2014).

Atendendo à natureza da prova digital, não existem fronteiras físicas que a restrinjam, em vez disso, esta prova está sujeita ao princípio da territorialidade, uma vez que pode ser armazenada em servidores em diferentes países, o que torna evidente a necessidade da cooperação internacional, prevista na LCC (Hermeiro, 2023).

Santos (2005) destaca as características singulares deste meio de prova face aos tradicionais, a prova digital apresenta-se como mais vulnerável e complexa que as restantes, pois pode ser facilmente modificada. Esta prova carece de técnicas específicas para a sua recolha, e impõem necessidades de investigação céleres com instrumentos adequados.

A vasta quantidade de dados e a efemeridade dos mesmos comprometem a investigação. A conservação dos dados ocorre por um período limitado, de acordo com o art.º 2, alínea c) da LCC. A prova digital é volátil, pode ser eliminada e ocultada do seu suporte digital, o que dificulta a sua recuperação, e faz com que só seja possível fazê-lo a

[2] *Fruits of the poisonous tree doctrine*, segundo Andrade (1992), refere-se a uma metáfora jurídica que expressa a ideia de que, se a árvore, i.e., a prova tem uma origem ilícita, tudo o que dela deriva também o será. Todas as provas obtidas através de uma prova ilegal, não serão admissíveis no processo.

partir de ferramentas forenses. No entanto, a prova digital pode ser mais facilmente recuperável do que a prova física. Tanto o transporte como o armazenamento da prova, devem preservar a integridade da prova. Se estas etapas não forem respeitadas, a admissibilidade da prova em tribunal pode ser comprometida, bem como a apresentação dos elementos indispensáveis para o julgamento (Santos, 2005).

1.7. Princípios orientadores da prova digital

Os princípios que aqui iremos elencar, estão relacionados com as dificuldades da natureza da prova digital, e servem como orientações e pilares essenciais para esta prova.

A prova digital está subordinada à CRP, e como tal, ao princípio da integridade, confiabilidade e imutabilidade da prova (Meireles, 2023).

Esta prova segue os princípios basilares constitucionais. Desta forma, deve ser garantido o princípio da legalidade, no sentido em que se coadune com os direitos fundamentais do visado e que preencha os requisitos do princípio da proibição do excesso e os seus corolários (os subprincípios da necessidade, adequação e proporcionalidade em sentido estrito) e o princípio da subsidiariedade, no sentido em que só devemos utilizar medidas mais invasivas quando os mesmos resultados não possam ser garantidos com meios menos intrusivos. “O princípio da garantia e defesa dos interesses do cidadão ou dos seus direitos fundamentais” (Valente, 2004 p. 55).

O princípio do interesse público na realização da justiça tem valores a si associados, que realçam a integridade da prova digital, observa a legalidade material e formal dos métodos de obtenção de prova e regula a atividades dos atores judiciários, para garantir a confiança de todos os cidadãos na realização da justiça, e neste caso, no conteúdo fidedigno da prova. A este princípio conjuga-se como um limitador à sua esfera, o princípio do respeito dos direitos e interesses legítimos dos particulares (Meireles, 2023).

O princípio da boa fé é um instrumento que gere as expectativas dos particulares, protegendo os seus direitos e a sua confiança no Estado (Pinheiro & Fernandes, 1999).

Valente (2021) afirma que o princípio da boa fé é “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 criminal” (p. 60). O princípio da boa fé e da transparência, defendem que ambas as partes devem ter acesso à prova digital,

e podem contestar eventuais irregularidades, as decisões judiciais devem ser fundamentadas e a cadeia de custódia da prova deve permitir que o perito possa reconstituir os factos (Clemente, 2022).

Almeida (2018) constata ainda o princípio da auto-responsabilidade das partes, este está implícito na produção da prova, em que os intervenientes devem sustentar a responsabilidade pelos seus erros, e as consequências da sua negligência.

Reale (2010) relativamente aos princípios da prova digital, afirma que se interligam com os princípios constitucionais "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" (p. 60).

Os princípios da identidade e autenticidade da cadeia de custódia da prova, no qual deve ser garantido que não exista adulteração dos dados, contam com um registo detalhado de todos os procedimentos e percursos da prova digital, desde a sua recolha até à sua apresentação em tribunal. A cadeia de custódia da prova digital deve ser regida com base no respeito pelos princípios constitucionais, e a sua violação inquina a utilização da prova no processo (Clemente, 2022).

O princípio da indisponibilidade das competências ou da fixação da competência, estabelece que as funções desempenhadas ao longo do processo de recolha e preservação da prova devem ser exercidas pelos órgãos competentes. Este princípio reforça a distinção entre os OPC's e a função do perito, pois os primeiros não possuem competências para realizar exames ou perícias. Existem atos reservados à atuação dos peritos, nos termos do art.º 151.º do CPP (Clemente, 2022).

A prova pericial tal como consta no art.º 151 do CPP é necessária quando os factos carecem de uma apreciação proveniente de um conhecimento técnico específico. Quando o julgador entende que a matéria dos factos contém elementos de elevada complexidade de perceção, os peritos podem elaborar um relatório, cuja finalidade será ir ao encontro da verdade material (Almeida, 2018).

Também especialmente relevante no campo da prova digital é o princípio da jurisdicionalidade presente no art.º 20.º, n.º 4, CRP e no art.º 6.º da Convenção Europeia dos Direitos Humanos. Segundo este princípio há uma exigência de uma determinação, ordem ou autorização judicial prévia, atendendo à afetação dos Direitos fundamentais dos visados na realização de diligências processuais (Clemente, 2022).

Capítulo II. O regime jurídico da prova digital

2.1 O enquadramento internacional da prova digital

A Lei n.º 109/91, de 17 de agosto, conhecida como a Lei da Criminalidade Informática, foi a primeira legislação a nível nacional, dedicada a combater a criminalidade informática, contempla desde logo no capítulo II (os crimes ligados à informática) onde os art.º(s) 5.º ao 10.º concentravam as variadas tipologias informático-criminais. Esta Lei de 1991 tinha sido inspirada na Recomendação n.º R (89) 9 do Conselho da Europa, de 13 de setembro (Verdelho, 2009).

Considerando que esta Lei abrangia um limitado espectro de tipologias criminais, relacionadas com o crime informático e que se revelava desadequada ao novo paradigma social e à complexidade dos novos crimes informáticos, tornou-se evidente o seu carácter obsoleto. A rápida e significativa evolução tecnológica e científica, que ocorreu desde então, transformou profundamente a realidade e a criminalidade digital, tornando imperativa a adoção de um quadro normativo mais abrangente e adequado aos desafios emergentes da cibercriminalidade (Morim, 2022).

A CCiber também conhecida como a Convenção de Budapeste foi impulsionada pela ideologia de 1997[3] e a 23 de novembro de 2001 foi finalmente aprovada, fruto da criação conjunta entre os Estados membros do conselho da europa e os restantes Estados signatários. Tendo em conta que a cibercriminalidade praticada contra sistemas de informação é também uma ameaça contra os Estados, os serviços e contra a própria sociedade, carecia de uma resposta rápida e eficaz. Deste modo, este Tratado teve a finalidade de combater, a nível internacional, a criminalidade praticada por meio de sistemas informáticos (Fidalgo, 2019).

A CCiber trata-se de um documento de direito internacional público que foi fruto de um trabalho conjunto de vários peritos, com o intuito de harmonizar e complementar a legislação existente sobre esta matéria (Verdelho et al., 2003). Quanto à sua estrutura, a Convenção contempla 4 capítulos, o I capítulo é relativo a terminologias e definições sobre crimes informáticos e sistemas e dados. O II capítulo é relativo a disposições processuais e medidas a adotar a nível nacional. O III capítulo aborda os princípios gerais relativos à cooperação internacional e regula os mecanismos de assistência entre os

[3] O impulso jurídico dos EUA de 1997, pelos Estados-membros do Conselho da Europa, fomentou uma ideologia que deu origem ao início da redação da Convenção sobre o Cibercrime.

Estados para a investigação deste tipo de crimes e a preservação da prova. Por fim, o IV e último capítulo contempla as disposições finais (Cf. Resolução da Assembleia da República n.º 88/2009, aprova a CCiber, adotada em Budapeste em 23 de novembro de 2001).

Para fazer face às preocupações derivadas do terrorismo, após os acontecimentos do 11 de setembro de 2001, a União Europeia começou a defender que as investigações dos crimes terroristas deveriam ter mais margem para atuação e inclusive, caso necessário, as autoridades deveriam intervir nas telecomunicações, sem autorização judicial prévia. Começaram desde então, a apostar mais na investigação e no combate à criminalidade organizada. Foi neste âmbito aprovada a Lei n.º 5/2002, de 11 de janeiro, que "Estabelece medidas de combate à criminalidade organizada e económico-financeira", Lei que institui um regime para a recolha de prova e quebra de segredo profissional (Ribeiro, 2015).

Posteriormente surgiu a Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro, criada no âmbito do combate a ataques contra sistemas de informação, continha o objetivo de proporcionar a cooperação entre as demais autoridades nacionais e internacionais. Atendendo a que os sistemas informáticos representam a organização vital dos Estados, deu-se a crescente necessidade de implementar uma proteção eficaz contra qualquer tipo de ataque cibernético. Foram estabelecidas sanções (Cf. o art.º 6.º) proporcionais e respeitadoras dos direitos fundamentais, bem como, dos princípios elencados no art.º 6.º do Tratado da União Europeia que foram posteriormente, incorporados na Carta dos Direitos fundamentais da União Europeia, de 7 de dezembro de 2000. Estas sanções foram acordadas pelos Estados-Membros para os ilícitos elencados nesta Decisão-Quadro (Morim, 2022).

Apesar deste normativo ainda não abranger disposições de natureza processual penal[4] garantiu ainda que, os Estados membros da União Europeia adaptassem a sua matéria legislativa à anterior Convenção de Budapeste (Cardoso, 2018; Mesquita, 2010).

A Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro foi substituída pela Diretiva 2013/40/EU do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, sofrendo alterações significativas e essenciais face à anterior. Desde logo contou

[4] Apesar de ter incluído conteúdo penal substantivo, nomeadamente definições de tipologias criminais e a sua respetiva sanção, não contempla nem regula procedimentos penais, como a recolha ou a apreensão da prova.

com uma expansão das definições de crimes informáticos e foram adotadas medidas para fortalecer a cooperação entre os Estados-Membros (Morim, 2022).

A Diretiva n.º 2006/24/CE, do Parlamento e do Conselho, de 15 de março, havia sido aprovada imediatamente, no sentido de dar resposta aos atentados terroristas de londres (Lopes & Cabreiro, 2006). Este diploma é também referente "à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações" (Militão, 2012 p. 26).

A Lei n.º 32/2008, de 17 de julho, é "relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações". Esta Lei "transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho." (Cf. Lei n.º 32/2008, de 17 de julho).

A Lei n.º 32/2008 é em determinadas situações complementar à LCC, no que toca a investigação e repressão de crimes graves, mas garantindo sempre um equilíbrio entre a procura pela verdade e os direitos fundamentais.

A Lei n.º 41/2004, de 18 de agosto, que "transpõe para a ordem jurídica a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas" proíbe a revelação do conteúdo das comunicações, no âmbito da investigação feita através da Lei n.º 32/2008 (Cf. art.º 1.º da Lei n.º 32/2008).

Os fornecedores de serviços de comunicações eletrónicas procedem à transmissão de dados conservados às autoridades competentes, para fins de investigação. No entanto, esta autorização apenas pode ser solicitada pelo MP ou pela APC competente (Cf. art.º 9.º n.º 2 da Lei n.º 32/2008). Tal transmissão de dados, depende ainda de despacho fundamentado pelo juiz de instrução, se for elemento indispensável para o apuramento da verdade, ou para a prova. (Cf. art.º 3.º e 9.º da Lei n.º 32/2008). O legislador definiu no art.º 6.º da mesma Lei, que o período de conservação dos dados deve ser de "um ano a contar da data da conclusão da comunicação", enquanto que na Diretiva n.º 2006/24/CE, o art.º 6.º previa que os dados "deveriam ser conservados por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação" (Cf. art.º 6.º da Diretiva n.º 2006/24/CE).

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

Decorrente da evolução da criminalidade e do *modus operandi* associado ao avanço tecnológico, tornou-se irrefutável a necessidade de alterar o quadro legislativo, tornando-o adaptável aos novos desafios (Fidalgo, 2019).

Face à necessidade de criar um regime de recolha da prova em ambiente digital, capaz de dar resposta à cibercriminalidade e ser incisivo na realidade do novo século, foi criada a Lei n.º 109/2009, de 15 de setembro, que aprova a LCC, relativa a ataques a sistemas de informação que, também regula o acesso e a pesquisa de dados informáticos e a sua apreensão, quando se revelarem fundamentais para a descoberta da verdade ou para a prova (Cf. Lei n.º 109/2009, de 15 de setembro de 2009).

A entrada em vigor desta Lei, veio revogar a Lei da Criminalidade Informática (Morim, 2022).

A LCC impulsionada pelo direito europeu, a partir da Decisão-Quadro 2005/222/JAI, do Conselho, de 24 de fevereiro e da Convenção do Cibercrime, densifica numa só Lei as normas relativas à criminalidade em ambiente digital, e consagra também as normas relativas aos ataques contra os sistemas de informação. Esta Lei contempla as normas referentes à cooperação internacional em matéria penal e também criou tipologias criminais e exceções às regras gerais do CPP (Verdelho, 2009).

Portugal ratificou a CCiber, através da Resolução da Assembleia da República n.º 88/2009, de 15 de setembro, ano em que foi também aprovada a Lei n.º 109/2009, de 15 de setembro, que se propôs a cumprir os compromissos internacionais aos quais o Estado português se vinculou nesta Convenção. A LCC foi criada com o propósito de transpor para a ordem jurídica interna, as obrigações deste Tratado de direito internacional (Ribeiro, 2015).

A LCC foi o resultado da criação de adaptações a normas tradicionais do CPP, aplicadas ao ambiente digital. O melhor exemplo disso é a pesquisa de dados informáticos, que consta no art.º 15, como adaptação do regime das buscas, que integra o capítulo II do CPP e que, aplica os pressupostos do art.º 174.º CPP a esta Lei (Fidalgo, 2019).

A LCC é constituída por 5 capítulos, em que o primeiro se refere ao "Objeto e definições", o capítulo II "Disposições penais e materiais", onde incluem as infrações no âmbito do cibercrime do art.º 3.º ao 10.º. No capítulo III, "Disposições processuais", foram criados meios processuais específicos para crimes informáticos e outros traduzem-

se em figuras adaptadas do CPP ao ambiente digital. No capítulo IV da "Cooperação internacional" que contém as regras de colaboração entre as autoridades competentes no combate ao cibercrime, e o V capítulo sobre "Disposições finais e transitórias" (Morim, 2022).

No art.º 11 da LCC, está expressamente consagrado que, as disposições processuais previstas no capítulo III não prejudicam a aplicação da Lei n.º 32/2008, de 17 de julho, relativa à "conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas" para fins de investigação (Fidalgo, 2019). A Lei n.º 32/2008, regula dados de tráfego e de localização, identifica os utilizadores mediante o registo dos dados informáticos (Correia, 2014).

O Ac. do TRE de 20-01-2015 (Processo n.º 648/14.6GCFAR-A.E1), refere que a entrada em vigor da LCC, veio revogar tacitamente o exposto nos arts.º 187º a 190º do CPP, no que se referia à extensão dos mesmos a crimes informáticos, e a outras provas eletrónicas. Este Ac. defende que, quando a prova digital já está preservada em sistemas informáticos, deve-se aplicar o disposto nos art.º(s) 11 a 19 da LCC. Neste Diploma legal, surgem dois regimes distintos, o primeiro, que abrange os art.º(s) de 11.º a 17.º, e o segundo contempla os art.º(s) 18 e 19. O primeiro regime processual é classificado por este Ac. como o regime geral do cibercrime e da prova eletrónica.

Este primeiro regime, tal como defende Correia (2014) aplicam-se aos crimes informáticos que a mesma prevê no capítulo II, mas também a todos os crimes que careçam de recolha de prova em suporte eletrónico. Passando desde a sua entrada em vigor, a configurar um regime essencial no que à recolha da prova digital diz respeito.

O legislador contempla na LCC um regime geral referente a dados informáticos, sempre que for necessária a recolha de prova em suporte eletrónico, incluindo todos os procedimentos efetuados desde a preservação de dados (Cf. art.º 12 LCC), a pesquisa de dados informáticos (Cf. art.º 15 LCC) e a recolha e apreensão dos dados informáticos (Fidalgo, 2019).

Relativamente à preservação da prova digital, está contemplado no art.º 12.º da LCC que é da competência da AJ ordenar, sempre que seja de interesse para a produção da prova ou para a descoberta da verdade, que os dados informáticos específicos sejam preservados pelo fornecedor dos serviços e armazenados para posterior análise e tratamento, sobretudo se houver o receio de que esses dados se percam, se alterem, ou deixem de estar disponíveis. São também competentes para tal os OPC' s, em casos de *periculum in mora*, e devem os mesmos informar, no mais curto prazo de tempo a AJ

competente, transmitindo-lhe o relatório onde mencionam as investigações levadas a cabo, e os resultados das mesmas, bem como a prova recolhida e a descrição dos factos, (Cf. o art.º 253.º do CPP). Os OPC' s ficam neste âmbito, com o dever de sigilo, de cumprir os prazos e a respeitarem as ordens e os requisitos para o armazenamento destes dados (Almeida, 2018).

A pesquisa dos dados informáticos, que surge no art.º 15. º da LCC, transpõe para o direito português o conteúdo do art.º 19.º da Convenção de Budapeste, "Busca e apreensão de dados informáticos armazenados". A pesquisa de dados informáticos pretende conciliar os procedimentos processuais da pesquisa de dados contidos em sistemas informáticos, suscetíveis de conterem elementos indispensáveis para a produção da prova, e para a descoberta da verdade. Neste caso, a competência para ordenar ou autorizar esta pesquisa, é da AJ competente, i.e., o magistrado do MP na fase de inquérito, ou o juiz do processo, aquando da instrução ou julgamento. Também pode nos casos determinados pelo n.º 3 do mesmo artigo, a diligência ser realizada pelos OPC's, sem autorização prévia da AJ (Venâncio, 2023).

Face ao descrito, Rodrigues (2009) refere que estes tipos de pesquisas informáticas se materializam em duas fases, a primeira é "a descoberta e identificação dos repositórios eletrónico-digitais ou sistemas informáticos onde se situa a prova digital e, num segundo momento trata-se de identificar o tipo de informação digital aí contida". (p. 569) Estes repositórios são em alguns casos apreendidos para sobre eles ser realizada perícia e análise informática, em situações que tal não seja possível apenas é realizada uma duplicação da prova (Rodrigues, 2009).

O segundo regime previsto na LCC, decorre dos art.º(s) 18.º e 19.º e contempla no art.º 18.º n.º 1, um catálogo de crimes em que é admissível o recurso a interceção de comunicações, em tempo real. A diferença substancial entre ambos os regimes está no momento em que as comunicações se efetuam, o primeiro regime trata os dados já armazenados, enquanto que este segundo regime é referente a comunicações que se encontram em curso. Só se aplica a este segundo regime, a remissão feita para os art.º(s) 187º, 188º e 190º do CPP, em tudo aquilo em que não contrariarem a LCC (Cf. Ac. do TRE de 20-01-2015).

Tanto o art.º 18.º como o art.º 19.º da LCC, pela suscetibilidade dos mesmos afetarem de forma mais intrusiva os direitos fundamentais dos visados, não se submetem às disposições processuais do art.º 11.º da mesma Lei (Morim, 2022).

De acordo com o Ac. do TRE de 20-01-2015, existem diferentes catálogos de crimes presentes em diversas Leis, que condicionam o uso de dados informáticos, uma vez que a sua utilização está restrita a certos crimes que justificam o uso de medidas mais intrusivas. O art.º 11.º da LCC contempla os crimes que permitem a preservação de dados informáticos, o art.º 18.º do mesmo diploma legal é referente a crimes que permitam a obtenção de dados de tráfego e outros dados relacionados a crimes informáticos e a crimes previstos no art.º 187.º do CPP. O art.º 3.º da Lei n.º 32/2008, permite o acesso a dados conservados, para fins de investigação, apenas para crimes graves.

A Lei n.º 32/2008 tem um âmbito de aplicação restrito a dados que são obrigatoriamente armazenados por Lei, durante um determinado tempo, ao passo que, a LCC trata os dados preservados, ou seja, quando as autoridades ordenam ao fornecedor de serviços que preserve os dados com valor probatório em que exista o risco de se perderem, serem alterados, ou deixarem de estar disponíveis (Cf. Ac. do TRE de 20-01-2015).

Já o art.º 19.º da LCC que determina as ações encobertas no decurso de inquérito para os crimes previstos no seu n.º 1, aplicam-se às mesmas o regulamentado para a interceção de comunicações (Cf. art.º 19.º da Lei n.º 109/2009, de 15 de setembro).

No entanto, a remissão ao CPP não é extensível aos restantes artigos da LCC, uma vez que o CPP não abrange especificamente crimes informáticos e, para esse contexto, é a LCC que define os procedimentos específicos a adotar (Fidalgo, 2019).

Em síntese, no ordenamento jurídico português, ao nível do tratamento dos dados informáticos, existe uma articulação entre diversas fontes normativas, a Lei n.º 32/2008, a LCC, o CPP e a CCiber. A aplicabilidade de cada regime processual depende de três fatores fundamentais, a natureza dos dados (preservados ou conservados), o tipo de crime investigado de acordo com o catálogo de crimes aplicável e a finalidade do acesso aos dados.

2.3. Lei do Cibercrime, enquanto Lei extravagante

Cabe referir que não existe no CPP um regime específico direcionado para a recolha e tratamento de provas em suporte eletrónico, em vez disso, este diploma contempla no título III "Meios de obtenção de prova", livro III "Prova", capítulo IV "Das escutas telefónicas", os artigos 189.º e 190.º, que fazem a extensão a outras formas de comunicação, conversações ou transmissão de dados, mesmo que a partir de um suporte

digital, ao regime das escutas telefónicas, optando o legislador por fazer uma remissão para os artigos 187.º e 188.º do mesmo regime. (Cf. DL n.º 78/87, de 17 de fevereiro).

O art.º 187.º do CPP para o qual é feita esta remissão, tem a epígrafe "Admissibilidade" e o art.º 188.º sobre "Formalidades das operações" determinam ambos o regime jurídico da interceção e gravação de conversações ou comunicações telefónicas. Estes artigos obedecem a uma série de parâmetros, perante os quais, sob pena de nulidade, transportam a obrigação de seguir os pressupostos e as condições materiais e formais elencadas. Porém, ambos os artigos estão pensados para as escutas telefónicas como meio de obtenção de prova e não concretamente para a prova digital (Fidalgo, 2019).

Almeida (2018) refere que as exigências de uma prova digital ou das escutas telefónicas são diferentes, e não devem ter os mesmos pressupostos nem as mesmas exigências normativas. Garante ainda que, utilizar o mesmo regime jurídico para ambos os meios de prova, pode trazer problemas, sobretudo acerca da sua admissibilidade. O que ocorre neste caso, à luz do CPP é que este diploma aplica para diferentes meios de prova, a mesma "admissibilidade, requisitos e pressupostos das interceções das escutas telefónicas" (Almeida, 2018, p. 46).

Desde a entrada em vigor da LCC, que os art.º(s) 187.º a 190.º do CPP não são a resposta adequada para a recolha de prova eletrónica, pois esse passou a ser o objeto da presente Lei (Cf. o art.º 1º da LCC) (Fidalgo, 2019).

À semelhança do evidenciado por esta autora, também o Ac. do TRE de 20-01-2015 (processo n.º 648/14.6GCFAR-A.E1), defende que desde a entrada em vigor da LCC, que os referidos art.º(s) do CPP deixaram de ser aplicáveis por extensão a telecomunicações eletrónicas, crimes informáticos, e à recolha da prova digital.

A LCC aplica-se para os crimes nela previstos, crimes cometidos por meio de sistemas informáticos, e crimes em que seja necessário proceder-se à recolha de prova em suporte digital (Correia, 2014). Porém, este regime é aplicável de um modo geral a todos os crimes, independentemente de serem ou não, cometidos através de sistemas informáticos, desde que a prova digital a ser recolhida no âmbito desse crime, seja relevante para a investigação do mesmo (Almeida, 2018).

O legislador ordinário manteve a decisão da não inserção das normas da LCC no CPP, optando por fazer da LCC uma Lei extravagante, que regula especificidades da recolha da prova digital, sem integrar o CPP (Morim, 2022).

Fidalgo (2019) afirma que a LCC é um regime que orienta a recolha de provas digitais e dados informáticos, sejam elas referentes a cibercrimes ou a outro tipo de

criminalidade. Assim, sobretudo o regime geral do cibercrime e da prova eletrónica (Arts. de 11.º a 17.º da LCC) poderia estar tipificado no CPP, uma vez que este é o principal diploma que regula as normas processuais. Desta forma, existiria mais coerência e harmonia entre o CPP e a LCC. Dado que o CPP já contém normas sobre a interceção de comunicações e apreensão da correspondência, a mesma autora defende que, faria mais sentido incluir também neste diploma, uma abordagem ao regime geral da recolha da prova em ambiente digital (Fidalgo, 2019).

Esta perspetiva é especialmente pertinente se tivermos em conta que o CPP contempla no Livro III "Da prova" os vários meios de prova existentes, mas não regula a prova digital. Ao manter a LCC fora do corpo normativo do processo penal, o legislador pode ter contribuído para uma fragmentação que, pode dificultar a aplicação prática e coerente da lei. Por sua vez, equiparar o regime das escutas telefónicas ao regime da prova digital é ignorar a complexidade técnica e a ambiguidade do ambiente digital, uma vez que os requisitos legais das escutas telefónicas foram pensados para uma realidade distinta, como sublinha também Almeida (2018). Desta forma, defendemos que se evidencia aqui uma falta de sistematização nesta opção do legislador, que não confere uniformidade a esta prova em relação às restantes.

Correia (2014) assevera ainda que, existem para a mesma realidade, três diplomas diferentes (CPP, LCC e Lei n.º 32/2008) e esta decisão do legislador, provoca assimetria e a descentralização do CPP, para uma prova que é tão crucial na atualidade, aplicando para tal uma dispersão de diplomas legais. O mesmo autor refere que um diploma bem estruturado seria suficiente "*leges nom sunt multiplicandae sine necessitae*" (p.55).

Neste sentido, tanto a Lei n.º 32/2008 quanto a LCC reduziram a abrangência do art.º 189.º do CPP, que anteriormente se aplicava a diversas formas de recolha da prova digital. Vieram ambas privilegiar o particular, em vez do geral, para não se alterar o CPP, fazendo com que o regime essencial da prova digital seja encontrado na Lei extravagante. A Lei n.º 32/2008 apresenta um regime específico para a recolha de metadados, tornando o art.º 189.º menos relevante nesse contexto. Já a LCC define requisitos e regras próprias para a apreensão de dados informáticos, interceção de comunicações, ações encobertas, pesquisa de dados informáticos, incluindo a apreensão de correio eletrónico, que passou a ser regulamentada pelo art.º 17.º da LCC, restringindo ainda mais o âmbito de aplicação do art.º 189.º do CPP. Neste caso, ambas as Leis extravagantes referidas têm primazia face ao regime geral, que se encontra, nessa parte, tacitamente revogado (Correia, 2014).

Importa, pois, ressalvar que, tendo o art.º 189.º do CPP visto o seu âmbito de aplicação significativamente restringido com a entrada em vigor da LCC, considera-se que, no que respeita à apreensão de correio eletrónico enquanto meio de prova digital, o mesmo se encontra tacitamente revogado. Assim, no capítulo seguinte, analisaremos a aplicação do artigo 17.º da LCC, enquanto regime jurídico vigente para a apreensão deste tipo de prova.

Capítulo III. O correio eletrónico enquanto meio de prova

3.1. Conceptualização e enquadramento do correio eletrónico

Os capítulos anteriores foram dedicados à prova digital e à sua complexidade. A partir deste capítulo, o foco incidirá concretamente sobre o correio eletrónico, um meio de comunicação que assume um papel central na produção de prova nos processos da atualidade. Para estruturar esta análise de forma clara e fundamentada, começaremos por esclarecer neste ponto, o conceito de correio eletrónico, estabelecendo as bases necessárias para a compreensão do seu regime jurídico e das implicações da sua utilização como meio de prova.

> Na Grécia Antiga, cerca de 190 a.c., um general grego, para fazer anunciar a vitória que tinha alcançado em Maratona contra os Persas, enviou um dos seus soldados a Atenas incumbindo-o de tal missão. Este correu cerca de quarenta quilómetros para anunciar a boa nova, tendo chegado e balbuciado a palavra "vitória", falecendo nesse mesmo instante. Fontes históricas atribuem esta situação ao nascimento do termo *correio*, advindo precisamente da palavra *correr.* (Ramos, 2017, p. 9).

Em termos históricos, a troca de mensagens sempre foi fundamental para a evolução dos povos, esta forma de comunicação revela-se essencial até aos dias de hoje (Ramos, 2017).

O avanço tecnológico permitiu revolucionar as formas de comunicação, o correio eletrónico surgiu neste contexto como um instrumento essencial. A sua origem remonta aos finais dos anos 60, do século anterior, aquando da criação do primeiro computador. O veredicto que fomentou o impulso do correio eletrónico ocorreu em 1971, com a contribuição do programador norte-americano Ray Tomlinson. Com este valioso contributo, foi possível desenvolver um sistema que permitia enviar mensagens a partir de computadores distintos, ligados a uma rede informática chamada *ARPANet*[5] (Andrade, 2019).

[5] A *Advanced Research Projects Agency* Network foi uma rede de computadores criada para transmitir informações de cariz militar de conteúdo sigiloso.

O mesmo programador criou ainda o formato de *email* que conhecemos hoje, após compreender que o símbolo "@" significava *"at"* (num determinado lugar), e considerou ideal localizar este símbolo no endereço de *email*, entre o nome de cada usuário e a plataforma ou o servidor que permite essa comunicação. Esta foi a primeira rede de computadores, foi criada entre militares, como um programa de comunicação à distância, uma vez que o intuito era trocar informações confidenciais rapidamente e de uma forma segura (Ramos, 2017).

Foram criados protocolos para permitir a troca de mensagens pelos servidores de correio eletrónico, os "*simple mail transfer protocol*" e o "*post office protocol*" (Morim, 2022, p. 23).

Na atualidade, o correio eletrónico representa o sistema de comunicação mais usado a nível profissional, mas também a nível pessoal, as mensagens são recebidas pelo destinatário no mesmo momento em que são enviadas através da internet. Existem variados servidores, cada um com as suas condições de acesso, alguns exigem dados pessoais como o número de telefone, outros não. "Os critérios de acesso à realidade da prova digital, no caso de onde a mesma se extrai, terão que ser critérios ponderadores do seu tratamento jurídico e de força probatória." (Meireles, 2023, p. 109).

A definição de correio eletrónico encontra-se plasmada na Lei n.º 41/2004, de 18 de agosto, al. b) do n.º 1 do art.º 2.º. Segundo esta disposição, considere-se correio eletrónico "na redação que lhe foi dada pela Lei n.º 46/2012, de 29 de agosto, (…) 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" (Nunes, 2021, p. 331). Este meio de comunicação caracteriza-se pela sua natureza não presencial e pela rapidez na transmissão da informação (Nunes, 2021).

Ainda assim, a doutrina diverge quanto à uniformização do conceito de correio eletrónico. À semelhança da Lei anteriormente mencionada, Cardoso (2018) refere que estas mensagens contemplam dados de tráfego presente nos cabeçalhos, que incorporam tanto texto, como som, imagem, utilizando para tal, redes informáticas e sistemas de informação para emissão, receção e armazenamento.

Ramos (2017) acrescenta que o correio eletrónico é um programa que permite a comunicação instantânea entre o emissor e o recetor, independentemente do local onde se encontrem, e destaca a natureza eletrónica desta prova digital e informacional. Com a evolução tecnológica, deu-se a criação de novos serviços *webmail*, como é o caso do

Gmail, Hotmail, Yahoo, Sapo, entre outros. Foi ainda possível, face ao apuramento tecnológico permitir o acesso imediato à caixa de correio eletrónico em diferentes dispositivos móveis, desde o telemóvel, *tablet*, computadores...

A Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho define o correio eletrónico como qualquer mensagem que incorpore texto, voz, som ou com a forma gráfica, que seja enviada através de uma rede pública de comunicações, e que pode ser conservada numa rede ou no equipamento do destinatário, até este receber de facto a mensagem (Diretiva 2002/58/CE, art.º 2º, al. f)). O legislador transpôs esta diretiva para a LCC nos art.º(s) 2.º e 17.º, mas optou por não adotar nenhuma definição neste diploma para o correio eletrónico e registos de comunicações de natureza semelhante, pelo que se aplica logicamente a definição previamente estabelecida.

Casabona (2006) sugeriu uma definição para correio eletrónico como

> uma modalidade de comunicação, em geral de carácter pessoal, que incorpora texto, som e imagem e que se serve das redes telemáticas como tecnologia de transmissão e dos sistemas informáticos (computadores e o software ou sistema lógico correspondente) como instrumentos de emissão e receção entre dois ou mais comunicantes e nesse caso de armazenamento de mensagens (p. 129).

Ramos (2017) conclui que as características essenciais do correio eletrónico são "assíncrono, ubíquo, digital e informático" (p. 12). Destas definições quer o autor destacar a capacidade de o correio eletrónico ser acedido instantaneamente, sem a necessidade de se instalar no dispositivo, pode ser acedido a partir de diferentes locais, utilizando somente dados e informações digitais.

O art.º 17.º da LCC estabelece um regime específico para a apreensão do correio eletrónico e registos de comunicações de natureza semelhante, que pode ser entendida como mensagens em plataformas *WhatsApp, Skype, Sapo*… (Cardoso, 2018; Nunes, 2021). Este regime regula as comunicações recebidas e armazenas pelo sistema informático do destinatário, mas também fornece prerrogativas para a atuação das autoridades no âmbito da apreensão de comunicações durante a investigação criminal. Este artigo é uma adaptação do CPP no regime das apreensões ao ambiente digital. (Cardoso, 2018).

Ramos (2017) destaca que a natureza da prova obtida através da apreensão da correspondência tradicional é distinta da do correio eletrónico, sublinhando que a aplicação do mesmo regime jurídico para ambas levanta sérias incongruências. Segundo o autor, esse paradoxo legal tornou-se particularmente evidente com a entrada em vigor da LCC.

Do ponto de vista da informática, de uma forma sucinta, optamos por clarificar em que consiste o programa informático que nos dá acesso ao *email*, com base em Ramos (2017) a comunicação ocorre por *inputs* e *outputs* criados num sistema informático, resumindo-se a *bits* e *bytes*, que usam a combinação de dois dígitos "0" e "1" e é desta forma que se partilha a informação, mediante um sistema numérico binário. Este programa informático contém ainda um sistema de ficheiros que grava, guarda e copia informações e dados provenientes de comunicações, inclusive aquelas que foram já eliminadas dos dispositivos.

O art.º 17. º da LCC regula ainda a apreensão de registos de comunicações de natureza semelhantes, Cardoso (2018) refere que estes podem ser *SMS* (serviços de mensagens curtas), *EMS* (serviço de mensagens desenvolvido) e *MMS* (serviço de mensagens multimédia) e podem ser efetuados através do telefone, por *transmission control protocol*, associando-lhes um endereço IP. O mesmo autor acrescenta que podem ser enviadas mensagens instantâneas, que incluam áudio, videoconferências, textos e ficheiros que, a partir do momento em que são enviadas para o destinatário, ficam armazenadas e podem ser alvo de apreensão (Cardoso, 2018).

3.2. Procedimentos de Investigação Criminal: a identificação do endereço IP por consulta ao ISP, e a recolha de cabeçalhos técnicos de mensagens de correio eletrónico

Este tema dedica-se a dar conhecimento ao leitor dos procedimentos práticos da investigação criminal da PSP, no contexto da recolha de elementos que comprovem a integridade e autenticidade da correspondência eletrónica. A investigação criminal enfrenta desafios significativos, especialmente no que diz respeito à identificação dos utilizadores dos sistemas informáticos e à rastreabilidade do trajeto das comunicações do correio eletrónico. Aqui, iremos abordar dois dos procedimentos fundamentais neste âmbito: a recolha de cabeçalhos técnicos de mensagens de correio eletrónico e a

identificação do endereço IP, através da consulta dessas informações ao ISP (Fornecedores de Serviços de Internet).

Primeiramente há que compreender que todas as comunicações online geram um percurso que fica registado no histórico dos servidores e contempla todos os dados técnicos da comunicação. O núcleo de cibercriminalidade da PSP é o responsável pela recolha de cabeçalhos técnicos de correio eletrónico. Este processo permite o rastreamento da mensagem, mostrando todo o percurso do *email*, o que determina, com base nessa informação, se este é autêntico ou não. (Cf. Manual de Recolha de Cabeçalhos Técnicos de Mensagens de Correio Eletrónico).

Sempre que é feita uma comunicação no correio eletrónico, é criado um registo com toda a informação no cabeçalho do *email*. Este registo contempla todos os dados e informações, a partir do momento em que a comunicação chega à caixa de entrada do destinatário. A cada uso da rede, é associado um trajeto que agrega a informação relativa ao endereço IP. Cada *email* é enviado através de infraestruturas como, a *Simple Mail Transfer Protocol Session, Mail Exchange Record, WHOIS-databases, Passive Domain Name System.* (Cf. Manual de Recolha de Cabeçalhos Técnicos de Mensagens de Correio Eletrónico).

Ramos (2014) refere que estas infraestruturas são usadas para transferir as comunicações de um servidor para o outro. O mesmo autor relativamente aos cabeçalhos técnicos demonstra que, ficam registados diversos elementos essenciais, que atestam a veracidade e integridade do *email*. Ainda assim, na atualidade é possível ocultar alguma informação com recurso a servidores temporários, ou que ocultem estes cabeçalhos técnicos, desta forma os *email*s podem ter a duração de 10 minutos a 24 horas. Contudo, sempre que é solicitado ao ISP os registos técnicos, obtém-se as informações originais, que não podem ser alterados nem manipulados pelos utilizadores. E sempre que existirem suspeitas da possibilidade de existir manipulação de dados, pode ser requerida a preservação imediata dos dados técnicos, uma vez que o fornecedor dos dados é obrigado a mantê-los inalteráveis.

Os cabeçalhos técnicos são constituídos por metadados, nomeadamente o endereço eletrónico do remetente da mensagem, a data, hora e fuso horário em que o *email* foi enviado, onde consta uma identificação individual relativa à mensagem, o assunto do *email*, o endereço IP do dispositivo que foi conectado ao programa de *email*, que enviou a mensagem e o endereço eletrónico do destinatário. A Leitura dos cabeçalhos técnicos deve ser iniciada na parte final do seu conteúdo e após concluída a Leitura,

identifica-se o endereço IP do remetente e faz-se o rastreamento e identificação do utilizador. Com essa informação, consulta-se o ISP do servidor e solicita-se ao fornecedor de serviços, os elementos relativos à identificação do remetente (Cf. Manual de Recolha de Cabeçalhos Técnicos de Mensagens de Correio Eletrónico).

Verdelho (2004) afirma que todas as comunicações realizadas através da internet, assim como o percurso das mensagens no correio eletrónico entre o emissor e o recetor, permanecem registadas num histórico do servidor. Porém, estes dados registados, em nada dizem respeito ao titular do acesso à rede, à sua identidade ou ao conteúdo das informações. No âmbito de uma investigação, só quando solicitado aos fornecedores de serviços de internet os dados associados a um determinado utilizador, que acedeu a uma determinada hora, dia e local, onde o sistema está fisicamente instalado, é que é permitido o acesso à identidade associada ao endereço IP. Como as comunicações ficam armazenadas num registo que capta o seu percurso através da conexão à rede, estes dados podem ser relevantes para a investigação.

No entanto, os fornecedores têm recusado conceder o acesso a essas informações tanto ao MP como à PJ. Com base nesta recusa, está a alegação de que esse registo mostra apenas dados relativos ao tráfego e não confere nenhuma certeza relativamente ao conteúdo das comunicações entre o emissor e o recetor. Estes estão associados à faturação detalhada, permitindo rastrear as interações realizadas entre os utilizadores. Para o mesmo autor, a recusa dos fornecedores é indevida, e não existe nenhuma reserva à obtenção desses dados pelo MP ou pela PJ (Verdelho, 2004).

Neste sentido, Ramos (2014) argumenta que a interpretação da Lei não deve ser discutida pelos operadores de comunicações, e que estes devem cumprir as ordens legítimas provenientes dos magistrados competentes, pois caso ocorra alguma invalidade na prova, os responsáveis por aferi-la são os tribunais. Este autor vai mais além e afirma que a recusa dos fornecedores de serviços em prestar as informações solicitadas, configura o crime de desobediência, ao abrigo do art.º 14 da LCC.

3.3. A apreensão do correio eletrónico ou registos de comunicações de natureza semelhante: conflitos com direitos fundamentais

Durante uma investigação, a necessidade da apreensão de correio eletrónico ou registos de comunicações de natureza semelhantes pode representar uma ameaça significativa aos direitos fundamentais dos visados. Antes de mais, importa destacar que

os propósitos associados ao processo penal são a descoberta da verdade material, a realização da justiça, e a proteção dos direitos fundamentais do arguido e de terceiros envolvidos no processo (Morim, 2022).

O equilíbrio que se procura alcançar, entre a descoberta da verdade e a proteção dos direitos fundamentais é um desafio constante, frequentemente marcado por conflitos e tensões jurídicas complexas. Como sublinha Dias (1987) ao refletir sobre as finalidades do processo penal, este dilema é "antinómico e antitético" (p. 13), traduzindo-se numa tensão estrutural entre a eficácia probatória e as garantias fundamentais. A apreensão de correio eletrónico ou registos de comunicações de natureza semelhante é particularmente intrusiva na esfera da vida privada, na medida em que concede aos investigadores o acesso completo a informações pessoais e a mensagens apreendidas (Dias, 1987).

Entre os direitos fundamentais mais diretamente afetados encontra-se o direito da inviolabilidade de correspondência e comunicações, consagrado no art.º 34.º, n.º 1 da CRP, que proíbe a ingerência no domicílio, na correspondência e em outros meios de comunicação privada. Esta norma abrange implicitamente as comunicações eletrónicas, incluindo o correio eletrónico, por constituírem modalidades de correspondência sustentadas por telecomunicações (Canotilho & Moreira, 2007).

Este direito representa não apenas uma proteção da vida privada, mas também um mecanismo de salvaguarda da dignidade da pessoa humana, do livre desenvolvimento da personalidade e a liberdade individual. A sua restrição só pode ocorrer em situações excecionais previstas na lei e mediante uma rigorosa ponderação em conformidade com o princípio da proporcionalidade em sentido amplo, de acordo com a análise ao art.º 18.º n.º 2 da CRP (Canotilho & Moreira, 2007).

Outro direito fundamental relevante é o direito à autodeterminação informacional que, à luz do art.º 35.º da CRP protege o tratamento de dados pessoais e informacionais sobre os cidadãos, impede qualquer violação de informações de índole pessoal e o seu aproveitamento abusivo (Neves, 2011). Assegurando que cada indivíduo mantém o monopólio das suas próprias informações, evitando ser reduzido a um mero "objeto de informações" (p. 551). Paralelamente, o art.º 26.º da CRP consagra o direito à reserva da intimidade da vida privada e familiar, também vulnerável à intrusão associada à apreensão de correio eletrónico (Canotilho & Moreira, 2007).

Influenciada pelo pensamento jurídico alemão, a doutrina portuguesa tem acolhido a Teoria das Três Esferas, segundo a qual a proteção da vida privada se distribui em três níveis, a esfera íntima é composta pela saúde, sentimentos e sexualidade, a esfera

privada define o historial e informações relativas ao seu contexto social, e a esfera pessoal trata a vida inserida na sociedade e as interações públicas (Neves, 2011). Neste quadro, a apreensão de correio eletrónico pode atingir simultaneamente vários níveis, em especial a esfera pessoal e a privada, dada a natureza frequentemente sensível das informações armazenadas digitalmente.

O art.º 126.º do CPP concretiza o princípio constitucional da inadmissibilidade das provas obtidas por meios que violem direitos fundamentais, nomeadamente através da ingerência ilegítima na vida privada, na correspondência e nas comunicações. Este princípio tem respaldo no art.º 34.º da CRP, que consagra a inviolabilidade da correspondência e das telecomunicações, e no art.º 26.º do mesmo diploma, que garante a reserva da intimidade da vida privada e familiar (Andrade, 1992).

Como uma das garantias de processo criminal, o art.º 32.º n.º 4 da CRP estabelece que qualquer ingerência em direitos fundamentais deve ser autorizada por um juiz, e apenas os atos que não envolvam tais direitos, podem ser delegados em outras autoridades judiciárias (Albuquerque, 2011).

O Ac. do TC n.º 128/92, de 24 de julho, reconheceu expressamente que o correio eletrónico, à semelhança da correspondência tradicional, constitui uma expressão da vida pessoal e uma representação da vida privada e, como tal, merece igual proteção constitucional. Este entendimento tem sido reforçado pela doutrina, que sublinha que o conteúdo das mensagens digitais integra a esfera da vida privada e exige proteção jurídica reforçada, especialmente no contexto de investigações criminais (Neves, 2011).

Autores como Neves (2011) e Ramalho (2017) sustentam que, no contexto digital, a palavra adquire um valor constitucional intensificado, uma vez que, no ambiente digital as palavras são registadas, armazenadas e potencialmente disseminadas de forma duradoura, o que acentua a necessidade de uma proteção jurídica mais exigente.

A nível internacional, o art.º 8.º da Convenção Europeia dos Direitos Humanos garante o direito ao respeito pela vida privada e familiar, e estabelece limites rigorosos sobretudo no que concerne à ingerência das autoridades públicas na esfera pessoal dos indivíduos, concretizada no direito à privacidade. Este artigo baseia-se no fundamento de que a promoção da dignidade humana proíbe interferências injustificadas à sua privacidade, e se existir, deve ser plenamente justificada, proporcional, necessária e adequada a alcançar o objetivo em causa (Mendes, 2021).

O TEDH considera que o direito à privacidade, tal como consagrado no referido art.º 8, deve abranger também a proteção da informação digital, incluindo comunicações

eletrónicas como os *email*s. Esta interpretação amplia a proteção da privacidade ao contexto profissional, garantindo que as comunicações por *email*, entre outras formas de dados informáticos, sejam tratadas com a mesma salvaguarda conferida à correspondência tradicional. Esta proteção apresenta exceções, uma vez que em situações previstas na Lei e devidamente justificadas, pode haver intervenção das autoridades públicas no direito à privacidade, e à vida familiar e privada. Quando o TEDH tem que se pronunciar relativamente à violação deste artigo, tem que identificar se houve uma intromissão em algum dos direitos em causa, e se essa intromissão teve ou não legitimidade para acontecer, mediante uma norma habilitante. Por último, tem que verificar se houve proporcionalidade nas medidas adotadas, ou seja, se houve equilíbrio entre os direitos lesados e o interesse público da sociedade na realização da justiça (Mendes, 2021).

3.4. As implicações jurídicas da extensão legal impulsionada pelo art.º 189.º do Código de Processo Penal

A reforma legislativa de 2007, incluiu na sua atualização a disposição no art.º 189.º do CPP, com a epígrafe "Extensão" de uma remissão para os 187.º e 188.º do mesmo diploma, em que estes são aplicáveis a conversações ou comunicações transmitidas por qualquer meio distinto do telefone, nomeadamente o correio eletrónico, ou quaisquer outras formas de transmissão de dados por via telemática, (através de serviços de tecnologia informática) inclusive aquelas que estão armazenadas em suporte digital, i. e., para incluir no CPP a aplicação legal referente à prova digital, criou-se uma norma geral para a qual esta prova faz remissão. Não se encontra nestes artigos um regime específico para a prova digital (Almeida, 2018).

O art.º 189.º do CPP regula o regime jurídico aplicável à interceção e gravação de conversações ou correspondência eletrónica, conciliando os dois artigos anteriores (Fidalgo, 2019).

A revisão de 2007 provocou um aditamento ao art.º 189.º, em que se incluiu a alusão à prova digital, onde refere "mesmo que se encontrem guardados em suporte digital". O Juiz de direito Tiago Milheiro defende a revogação deste aditamento, uma vez que a LCC sugere a aplicação de outro regime[6]. (Morim, 2022).

[6] A parte final do art.º 17 da LCC remete para o art.º 179.º do CPP, aplicando ao regime da apreensão do correio eletrónico, o previsto para a apreensão da correspondência. No entanto, também o art.º 189.º do CPP prevê a

A grande controvérsia surgiu com a entrada em vigor da LCC, cujo art.º 17.º aplica à apreensão do correio eletrónico, o regime da apreensão da correspondência, art.º 179.º do CPP. Neste caso, a LCC acaba por revogar parcialmente e tacitamente o disposto no art.º 189.º ao aplicar às comunicações eletrónicas o regime previsto para as escutas telefónicas (Mesquita, 2010).

Para este caso, com base em Correia (2014), segue-se o princípio segundo o qual a *lex specialis derrogat legi generali,* e defende que o legislador deveria, após a entrada em vigor da LCC, ter formalizado a revogação parcial do disposto no art.º 189.º relativamente ao tipificado sobre a apreensão do correio eletrónico, uma vez que esse meio de obtenção de prova tinha sido regulado pelo art.º 17.º da LCC.

Rodrigues (2010) reforça que, desde a entrada em vigor da LCC, que a apreensão do correio eletrónico se tornou algo contraditório e complexo.

No âmbito dos direitos fundamentais, observa-se uma discrepância significativa no grau de intrusão e lesão entre o regime da apreensão da correspondência e o regime das escutas telefónicas. Ao passo que, o regime da apreensão da correspondência se refere a comunicações já efetuadas e armazenadas, o regime das escutas telefónicas trata de comunicações em tempo real. Perante esta diferença colossal na lesão de direitos que existe em ambos os regimes, entende-se que o regime das escutas telefónicas restringe de forma mais lesiva os direitos fundamentais dos intervenientes e sem o seu conhecimento, uma vez que se enquadram em métodos de investigação ocultos (Morim, 2022).

Entendemos que no âmbito do regime das escutas telefónicas ocorre uma monitorização em tempo real, uma ingerência imediata e contínua, a lesão da privacidade é ilimitada e a intimidade da vida privada é totalmente exposta. Para além de envolver terceiros, defende o princípio da proporcionalidade, que quanto mais invasiva for a medida, maior deve ser o controlo judicial e os critérios legais. Já uma comunicação efetuada através de um *email,* tem, na nossa perspetiva outras implicações, pois trata-se de uma comunicação armazenada, em termos do direito de autodeterminação informacional, o titular do conteúdo já exerceu o seu poder de controlo sobre a mesma, dado que a comunicação já foi enviada. Quanto à expectativa de privacidade do utilizador, a exposição da intimidade da vida privada não é imediata, a intromissão nos direitos de privacidade ocorre em relação ao passado das comunicações.

correspondência eletrónica e a submete ao regime das escutas telefónicas, o que gera uma contradição. Neste sentido, o juiz Tiago Milheiro defende que se devia retirar esta última inclusão do diploma processual penal.

Convém esclarecer que os métodos ocultos de investigação criminal utilizados nas escutas telefónicas são claramente mais lesivos porque ocultam do visado e neutralizam alguns direitos processuais, afetam terceiros, permitem recolher informações relativas ao seu histórico, e em tempo real (Ramalho, 2017).

Atendendo a esta dualidade de regimes contraditórios para a apreensão do correio eletrónico, em causa ficam os direitos fundamentais, dado que cada meio de prova tem as suas características, os seus critérios de necessidade e de proporcionalidade nos métodos de investigação e de obtenção da prova, consoante o art.º 18º, n.º 2 da CRP (Morim, 2022).

Em suma, a aplicação do regime das escutas telefónicas ao correio eletrónico suscita sérias reservas do ponto de vista da proporcionalidade, isto porque o regime das escutas foi concebido para comunicações em tempo real e pode afetar terceiros, o que o torna mais gravoso em termos de lesão de direitos fundamentais, como o direito à privacidade, à liberdade de expressão e ao contraditório (por assumir uma natureza oculta). Considerando que o correio eletrónico contempla comunicações já efetuadas e armazenadas, aproxima-se mais da correspondência tradicional.

Assim, aplicação do art.º 189.º do CPP ao correio eletrónico encontra-se especificamente nessa parte, tacitamente revogada. A entrada em vigor da LCC, ao estabelecer no art.º 17.º a aplicação do regime de apreensão da correspondência, previsto no art.º 179.º do CPP ao correio eletrónico, introduziu uma norma especial e posterior que prevalece sobre a norma geral anterior.

3.5. O regime jurídico da apreensão de correio eletrónico (art.º 17.º da LCC)

As mensagens de correio eletrónico e registos de comunicações de natureza semelhante, com o passar do tempo, têm vindo a ganhar mais importância no processo penal, afirmando-se como meios de prova essenciais (Cardoso, 2018).

Após mais de uma década da entrada em vigor da LCC, a prova digital continua a ser alvo de discussão em matéria de Processo Penal, sobretudo, porque a parte final do art.º 17.º desta Lei, faz remissão para o regime da apreensão da correspondência, previsto no CPP (Contardo, 2020). Leia-se neste artigo,

> quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema

> informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal. (Cf. art.º 17.º da LCC).

Assim, o regime da apreensão de correio eletrónico segue o modelo do regime da apreensão da correspondência, estabelecido no art.º 179.º n.º 1 do CPP. (Fidalgo, 2019).

Esta decisão do legislador, de remeter o regime da apreensão do correio eletrónico para o art.º 179.º do CPP, é criticada por diversos autores, por exemplo, Nunes (2021) defende que faria mais sentido, a sua equiparação ao regime das escutas telefónicas.

Importa salientar, que ao nível europeu, o legislador não atribuiu nenhum tipo de conexão entre o correio tradicional e o correio eletrónico, ao contrário do que acontece em Portugal no CPP (Ramos, 2017).

O Ac. do TRL de 11-01-2011, (processo n.º 5412/08.9TDLSB-A.L1-5) refere que, uma vez que o art.º 17. º da LCC remete para o regime da apreensão da correspondência, previsto no CPP, a aplicação deste regime deve ser efetuada na sua totalidade, sem redução do seu âmbito. Assim, com base neste Ac. as mensagens de correio eletrónico que tenham interesse para a descoberta da verdade ou para a prova, podem ser apreendidas com base no regime previsto no diploma processual penal. Consequentemente, sob pena de nulidade, tem que ser o juiz a primeira pessoa a tomar conhecimento do conteúdo das mesmas, ou determinar a sua imediata abertura pelos OPC's, em casos específicos.

À luz deste Ac., a aplicação total do regime de apreensão da correspondência à apreensão de correio eletrónico é, na perspetiva de Fidalgo (2019) contraditória, dado que o n.º 1 do art.º 179.º do CPP apresenta três requisitos para a apreensão da correspondência,

> a) A correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo
>
> que sob nome diverso ou através de pessoa diversa;

b) Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e

c) A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova (Cf. n.º 1 do art.º 179.º do CPP).

No entanto, estes três requisitos devem verificar-se cumulativamente, sob pena de se questionar a legalidade da apreensão. Fidalgo (2019) argumenta que o regime de apreensão da correspondência foi pensado para a correspondência tradicional e não se adapta adequadamente à natureza da correspondência eletrónica. A autora defende que destes três requisitos, apenas a al. c) se pode aplicar ao regime de apreensão do correio eletrónico. Com base nesta perspetiva, está a lógica da alínea a) pressupor que a correspondência ao ser "expedida" ainda se encontra em trânsito, o que é típico da correspondência física, mas não da correspondência eletrónica, que se encontra logo armazenada no servidor ou no dispositivo. Por sua vez argumenta também que a alínea b) não se aplica à correspondência eletrónica, porque contraria o art.º 17 da LCC, uma vez que este não exige moldura penal superior a 3 anos. O legislador, para o regime da apreensão do correio eletrónico, não colocou a necessidade de moldura penal superior a 3 anos, possivelmente, para garantir a eficácia da investigação digital, mesmo em crimes de menor gravidade, fomentando a recolha de provas digitais na investigação, a um número mais alargado de crimes (Fidalgo, 2019).

Apesar do Ac. do TRL de 11-01-2011, defender a aplicação integral do art.º 179.º do CPP, à correspondência eletrónica, esta abordagem suscita algumas dificuldades na prática, sobretudo ao nível da diferença da natureza e especificidade de ambas as provas. No nosso entender, à semelhança do argumentado por Fidalgo (2019), o legislador, ao redigir o artigo 17.º da LCC, optou deliberadamente por não exigir um limite de pena de prisão superior a três anos, para aumentar a eficácia da investigação de crimes digitais, mesmo os de menor gravidade, permitindo a recolha da prova digital em contextos mais alargados do que os casos previstos no regime da apreensão da correspondência. Divergimos da argumentação de Fidalgo (2019) quanto à inaplicabilidade da alínea a) à correspondência eletrónica. Entendemos que o critério relevante enfatizado pelo legislador não se trata do momento da expedição (que de facto assume contornos distintos na correspondência eletrónica), mas sim a titularidade do envio, ou seja, o facto de a

mensagem ter sido expedida pelo suspeito e dirigida a outrem, o que justifica, no nosso entender, a aplicação da alínea a) também neste contexto.

Clemente (2022) afirma que o art.º 179.º do CPP, foi concebido para a correspondência que ainda não foi entregue ao destinatário e que ainda se encontra em trânsito, apresentando-se como uma forma de interceção de comunicações. O regime da apreensão da correspondência, pressupõe a retirada da comunicação do circuito de transmissão, em tempo real, antes de chegar ao seu destinatário, impedindo a sua receção. Segundo o autor, esta lógica não se aplica diretamente à apreensão do correio eletrónico, uma vez que este diz respeito a comunicações já efetuadas e já recebidas pelo destinatário, ou àquelas que se encontram armazenadas no sistema informático acedido (Clemente, 2022). A nossa visão coaduna-se com esta perspetiva, uma vez que, as mensagens do correio eletrónico, por norma, já se encontram fora do circuito de transmissão no momento da sua apreensão, pois estão armazenadas no servidor do destinatário.

Este regime apresenta várias complexidades em termos de interpretação normativa, porque a remissão do art.º 17.º da LCC, para o regime de apreensão da correspondência, provoca a necessidade de equiparação entre a correspondência física aberta e lida pelo destinatário e o correio eletrónico recebido e lido, e a correspondência física não recebida nem lida pelo mesmo e o correio eletrónico não recebido e não lido. De acordo com a jurisprudência, quando aberta a correspondência física, esta é equiparada a um documento e não se enquadra no regime da apreensão da correspondência, mas sim no regime pensado para a prova documental (Nunes, 2021).

Passaremos agora a expor as diversas formas que o investigador tem de proceder à apreensão do correio eletrónico no decurso do inquérito. O art.º 17.º da LCC, permite que a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, se ajuste às especificidades de cada caso (Verdelho, 2009). Assim, podemos identificar três formas principais de apreensão:

A forma mais comum de apreensão do correio eletrónico ocorre quando o correio eletrónico é obtido no âmbito de uma pesquisa de dados armazenados em sistemas informáticos ou em suporte autónomo. Esta diligência requer uma autorização judicial para o efeito, nos termos do art.º 15.º n.º 2 da LCC, sob pena de nulidade e este despacho tem o prazo de validade máximo de trinta dias. Excecionalmente, também os OPC's podem proceder à pesquisa informática sem necessidade de um despacho prévio da AJ, no entanto, isto só pode ocorrer nos casos em que se obtenha o consentimento documentado de quem possuir o domínio desses dados, e em caso de "crimes de

terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa." (Cf. al. b) n.º 3 do art.º 15.º da LCC).

Esta diligência carece de comunicação imediata à AJ, conjuntamente com o envio do relatório previsto no art.º 253.º do CPP. Para a apreensão é necessário realizar uma cópia integral do sistema informático através da ferramenta forense. Posteriormente será o perito a analisar os dados apreendidos, que são submetidas à validação do MP no máximo em 72h, e o seu não cumprimento culmina numa irregularidade. Para além disto, é importante referir que existe um regime geral de apreensão de dados informáticos, que se encontra nos art.º(s) de 14.º a 16.º da LCC (Cardoso, 2018).

Além disso, o art.º 252.º do CPP, inserido no capítulo das medidas cautelares e de polícia é fundamental para demonstrar a competência dos OPC's na apreensão do correio eletrónico. Neste âmbito, a apreensão é transmitida ao juiz que tiver ordenado a diligência, se considerar que os elementos apreendidos são fundamentais junta-os ao processo (Cardoso, 2018). Nunes (2021) acrescenta que, para além disto, as mensagens do correio eletrónico são sujeitas a um exame por parte do JIC, e a falta deste exame, constitui uma irregularidade. Entendemos que este exame assume um papel essencial na salvaguarda dos direitos fundamentais dos visados, em que o exercício da competência do JIC no processo, garante que a ingerência nos direitos dos indivíduos seja submetida a um controlo judicial indispensável.

Esclarecemos desde logo que a realização da pesquisa informática, nem sempre é um requisito indispensável. Iremos agora a abordar a segunda forma que possibilita a apreensão do correio eletrónico, que ocorre quando os dados informáticos são entregues voluntariamente pelo visado às autoridades. Esta entrega voluntária confere às autoridades um acesso legítimo e dispensa a pesquisa informática. Existe ainda uma terceira possibilidade para se proceder à apreensão, que é de o visado juntar voluntariamente as mensagens ao processo, ou consentir na realização da pesquisa informática (Nunes, 2021).

Esta realidade tem sido comprovada juridicamente, como se pode ler no Ac. do TRL, de 29/03/2012, (Cf. processo 744/09-1S5LSB-A.L1-9) e no Ac. do TRP, de 22/05/2013 (Cf. processo 74/07.3PASTS.P1). Ambos os acórdãos demonstram que nem sempre o art.º 17.º da LCC se aplica a todas as formas de apreensão do correio eletrónico, especialmente em situações em que o titular dos dados informáticos consente na

disponibilização destes às autoridades, permitindo que sejam transcritos e anexados aos autos.

Por último, paralelamente, a doutrina debate as vantagens e desvantagens do uso de programas informáticos pelas autoridades para acederem diretamente aos sistemas informáticos dos visados[7] (Nunes, 2021). Contudo, esta discussão ultrapassa o objeto da presente dissertação. Podemos apenas sucintamente adiantar que, devido à característica imaterial da prova digital, os métodos científicos contemporâneos permitem a sua demonstração com base na Ciência Forense Digital e considerando as particularidades da investigação em curso e a gravidade dos ilícitos criminais, os meios tradicionais de obtenção de prova podem revelar-se insuficientes. Nestes casos, impõe-se o recurso a métodos ocultos de investigação criminal, que se apresentam como instrumentos eficazes na persecução da verdade material (Ramalho, 2017).

3.6. A Proposta de Lei de alteração ao regime da apreensão do correio eletrónico e o Ac. n.º 687/2021 do Tribunal Constitucional

Em 2021 houve uma tentativa de alteração à LCC, numa proposta de alteração da norma do art.º 17.º, com vista a clarificar o regime da apreensão do correio eletrónico. O legislador português pretendia pôr fim aos conflitos jurisprudenciais fruto deste artigo.

Esta proposta colocava no art.º 17.º, no n.º 2 uma permissão para os OPC's efetuarem apreensões sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada bem como, sempre que se verificassem situações de *periculum in mora*, contrariando o exposto no art.º 179.º do CPP.

Esta proposta adotou as posições de Verdelho (2004) e Cardoso (2018), que consideravam que não deveria ser o juiz o primeiro a tomar conhecimento do conteúdo das mensagens do correio eletrónico, alegando entre outros argumentos já abordados

[7] O *malware* é "um programa simples ou autorreplicativo que discretamente se instala em um sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade de sistema ou para assegurar que o utilizador seja incriminado por um crime informático" (Filiol, 2005, p. 83). O uso de *malware* como meio de obtenção de prova por parte das autoridades policiais, para acederem remotamente aos sistemas informáticos dos visados é um dos temas mais sensíveis e controversos da investigação criminal digital contemporânea. Têm-se intensificado os debates relativos á controvérsia jurídica e ética do uso destes programas informáticos. Importa sublinhar que o processo penal, enquanto instrumento de tutela dos direitos fundamentais, não pode prescindir de uma base legal clara e expressamente regulamentada para o uso deste tipo de programas. Contudo, surge na doutrina o entendimento que a admissibilidade de diligências tão intrusivas, apenas poderá considerar-se legítima quando autorizada por ordem judicial devidamente fundamentada e com respeito pelas exigências dos princípios constitucionais, sob pena de se colocar em risco o próprio Estado de Direito democrático (Junior, 2021).

anteriormente, razões de economia processual, de tempo, de competências informáticas e por ser prejudicial à investigação.

Como tal, a grande alteração substancial provocada por esta proposta conferia um papel primordial ao MP, sendo que lhe permitia que pudesse ordenar ou validar a apreensão do correio eletrónico durante o inquérito sem prévia autorização judicial, atendendo a que nesta fase, o MP é a autoridade competente.

É indiscutível a relevância do MP enquanto titular da investigação penal e parte fundamental na direção do inquérito, contudo, sempre que existe alguma afetação de direitos fundamentais esse papel deve caber, a nosso ver, obrigatoriamente ao juiz, por respeito do princípio de reserva juiz e para não existir uma subversão de papéis jurídicos.

Assim que o Presidente da República solicitou a fiscalização preventiva da constitucionalidade das normas, o TC, no Ac. n.º 687/2021, declarou a inconstitucionalidade das normas por unanimidade.

A verdade é que a proposta apresentada não resolveu dirimir os conflitos de interpretação normativa, nem construir um regime próprio que atendesse efetivamente às características das comunicações eletrónicas, enquanto prova digital com uma natureza própria. Tanto é que o n.º 6 do art.º 17.º desta norma, aplicava novamente o art.º 179.º do CPP, em tudo o que não se encontrasse previsto nos números anteriores.

Com base no descrito, afiançamos que esta proposta não se dignou a ter alterações essenciais, e concordamos com o Ac. n.º 687/2021 do TC. Não concordamos com a proposta apresentada, pois consideramos que não resolveu as contradições legais da remissão do art.º 17.º da LCC para o art.º 179.º do CPP. Reconhecemos que esta proposta pode abrir portas a interpretações que não devem ser feitas, que venham a permitir uma ingerência indevida às comunicações eletrónicas e até mesmo, dar aso a investigações indiscriminadas.

Também a Comissão Nacional de Proteção de Dados defendeu que o MP não tem a independência necessária para apreciar a necessidade de acesso ao conteúdo das comunicações e que essa deve ser a tarefa do juiz.

3.7. Apreciação Crítica ao regime da apreensão do correio eletrónico

A doutrina reforça a complexidade da interpretação destes regimes, na tentativa de harmonizar os normativos do CPP com a LCC. Questiona-se cada vez mais até que ponto o diploma penal é eficiente para lidar com os desafios e as complexidades

associadas à prova digital, sobretudo em investigações que exigem o acesso a dados armazenados em sistemas internacionais, como é o caso do correio eletrónico (Rodrigues, 2011).

Ambos os regimes acabam por colidir, uma vez que, para o regime da apreensão do correio eletrónico, o legislador transpôs os princípios processuais do regime de apreensão da correspondência, com as necessárias adaptações (Verdelho, 2009).

Após vários autores se oporem à coexistência formal dos vários regimes, que continuam necessariamente a ser articulados, expomos agora a nossa perspetiva.

Em primeiro lugar, é inegável que o correio eletrónico é um meio de prova fundamental nos processos da atualidade. O art.º 17 da LCC tem gerado debates doutrinários que criticam e expõem as fragilidades deste regime. Desde logo, a remissão da apreensão do correio eletrónico para as normas do art.º 179.º do CPP, torna a concomitância dos regimes complexa, também pela diferença na natureza das provas.

Acreditamos que o legislador não teve em consideração a natureza digital deste meio de prova, desde logo visível na inaplicabilidade integral do regime para o qual remete o art.º 17 da LCC, nomeadamente da al. b) do n.º 1 do art.º 179.º do CPP, que contraria o disposto na LCC ao restringir a recolha da prova a uma moldura penal concreta, o que não acontece na lei especial e por isso não pode ser aplicável. O mesmo se aplica relativamente ao n.º 3 do mesmo artigo, uma vez que a restituição referida no CPP não se coaduna com o regime da LCC, porque na correspondência tradicional a carta é retirada fisicamente do circuito de transmissão, mas na correspondência eletrónica apenas é feita uma cópia do suporte eletrónico.

Deste modo, partilhamos da opinião de Nunes (2021) e Cardoso (2018), relativamente a não se considerar adequado equiparar um *email* à correspondência física, isto porque, na nossa modesta opinião, o ambiente digital apresenta várias especificidades que devem ser tidas em conta e não se coadunam com os procedimentos efetuados em ambiente físico. Não sendo possível uma aplicação integral do regime para o qual remete a apreensão deste meio de prova, claramente porque o art.º 179.º do CPP foi concebido para correspondência física e não para correspondência eletrónica.

Em segundo lugar, a alteração do diploma processual penal que veio incluir na redação do n.º 1 do art.º 189.º do CPP a correspondência eletrónica, submetendo-a ao regime das escutas telefónicas, gera neste momento uma sobreposição legal. Não obstante à manutenção formal da disposição no CPP, entendemos, à semelhança do que tem sido sustentado pelos vários autores referidos, a extensão proposta pelo aditamento de 2007

ao CPP, no que toca à prova digital e em concreto ao correio eletrónico está, neste momento, obsoleta e apesar de se encontrar tacitamente revogada, deveria ser alvo de revisão e exclusão do regime.

Discordamos de Nunes (2021), quando refere que se deve equiparar o regime do correio eletrónico, às escutas telefónicas. Para além do já argumentado, defendemos que existe uma disparidade de afetação dos direitos fundamentais nos diferentes regimes, uma vez que, consideramos que as escutas telefónicas são um meio de obtenção de prova mais lesivo.

Em terceiro lugar, tanto o art.º 17.º da LCC como o art.º 179.º do CPP não são claros quanto à expressão "o juiz autoriza ou ordena" nem relativamente ao momento em que deve ser emitido o despacho judicial, e defendemos que tal deveria ser alvo de alteração e clarificação.

Por fim, o nosso entendimento é que deveria existir um regime específico para a apreensão do correio eletrónico, que não originasse zonas cinzentas, vazios legais nem desse margem para interpretações normativas tão divergentes, dado que, na prática, a articulação entre estes regimes se vê bastante complexa.

Para clarificar a nossa posição, procedemos a uma análise do regime jurídico em vigor, com o objetivo de identificar e interpretar possíveis soluções normativas adequadas à apreensão do correio eletrónico. O artigo 17.º da LCC, determina que apenas sejam submetidas à apreciação judicial as mensagens que se afigurem de grande interesse para a descoberta da verdade ou para a prova, o que pressupõe inevitavelmente, que exista uma triagem prévia das mensagens por parte dos OPC's, de forma a selecionarem apenas as que preencham esses critérios de necessidade da prova.

No entanto, esta triagem implica, ainda que parcialmente, a abertura das mensagens, pelo menos na medida necessária para verificar integralmente os remetentes e os destinatários da mesma, como critério de identificação das mensagens relevantes para a prova. Esta abertura, ainda que não implique a leitura do conteúdo das mensagens, pode levantar algumas dúvidas quanto à sua conformidade com os princípios da inviolabilidade das comunicações e da tutela judicial. Uma vez que o n.º 3 do mesmo artigo refere que "O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida".

Na prática, a simples abertura de um *email* do correio eletrónico, ainda que apenas para visualizar os cabeçalhos técnicos, os remetentes e destinatários pode já representar um grau de intromissão, que não está claro na letra da Lei. No entanto, essa

abertura técnica das mensagens pode ser, a única forma de realizar a triagem exigida pelo artigo 17.º da LCC, respeitando simultaneamente os critérios estabelecidos no artigo 179.º do CPP, nomeadamente no que diz respeito à identificação de mensagens expedidas ou recebidas pelo suspeito.

Assim, propomos que o legislador preveja expressamente uma distinção clara entre o acesso aos dados técnicos do cabeçalho do correio eletrónico, para efeitos de investigação, e a distinga da leitura do conteúdo da mensagem, permitindo que a primeira seja autorizada com menor exigência formal, salvaguardando, contudo, garantias essenciais de direitos fundamentais.

3.8. Distinção entre correio eletrónico fechado/não lido/ e aberto/lido

Atualmente, um dos grandes debates jurídicos relaciona-se com a aplicação do regime de apreensão da correspondência ao correio eletrónico. Entende-se que a principal dúvida gira em torno de saber se essa remissão abrange todas as mensagens de correio eletrónico, ou somente as que ainda não foram abertas nem lidas pelo destinatário.

Sistematizando o debate doutrinário, Andrade (2012) refere que, o que distingue a correspondência dos restantes escritos, é o facto desta se encontrar fechada, existindo um obstáculo físico à sua obtenção. A aquisição do conhecimento do seu conteúdo implica, neste caso, a rutura material e o seu extravio. O mesmo autor refere que caso uma carta tenha sido indevidamente aberta, e se encontre reservada em local pessoal, deixa de ser considerada uma carta fechada, ou seja, deixa de ser considerada correspondência. Pressupõe que, uma vez que a correspondência se encontra fechada é abrangida por uma tutela de sigilo, dado que nos deparamos com um obstáculo físico que delimita e protege o conteúdo da comunicação.

Apesar da entrada em vigor da LCC ter servido para dirimir complexidades e clarificar conceitos, a mesma veio causar divergência de interpretações face à apreensão do correio eletrónico. Isto por apresentar certas condições que podem requerer procedimentos diferentes, como o caso de as mensagens do correio eletrónico terem sido abertas e lidas, ou por outro lado, o destinatário ainda não ter tomado conhecimento do conteúdo das mesmas (Fidalgo, 2019).

A LCC não faz distinção entre as mensagens de correio eletrónico abertas e lidas e as não lidas, como resulta da leitura do Ac. do TRG, de 29/03/2011 (Cf. processo n.º 735/10.0 GAPTL-A.G1).

Contudo, existe alguma jurisprudência que faz a distinção entre estes conceitos. O Ac. do TRL, (processo n.º 463/07.3 TAALM), de 02/03/2011, para comparar o regime de apreensão da correspondência geral, previsto no CPP, à correspondência efetuada por meios telemáticos, refere que é necessário distinguir entre uma mensagem recebida e ainda não aberta, de uma mensagem recebida e aberta. Defende que as mensagens que já foram abertas pelo seu destinatário vêm o seu valor e o seu procedimento equiparado a documentos e, portanto, excluído do regime do art.º 17.º da LCC (Fidalgo, 2019).

Nunes (2021) fruto de uma interpretação aprofundada do art.º 17.º da LCC, afirma que a apreensão dos *email*s com base no regime do art.º 179.º do CPP, deve ocorrer apenas em casos em que, tanto o *email* como mensagens, tenham sido recebidas, mas o destinatário ainda não tenha tomado conhecimento do seu conteúdo. Para este efeito, Fidalgo (2019) salienta que as mensagens que ainda não foram abertas, ou seja, encontram-se por analogia, equiparadas a correspondência física fechada, é sigilosa e vê-se abrangida pelos direitos constitucionais presentes no art.º 34.º n.º 1 da CRP. Uma vez que as mensagens que ainda não foram abertas e lidas pelos destinatários, não foram descarregadas no seu sistema informático.

A complexidade associada à distinção entre o correio eletrónico aberto e lido e aquele que não é aberto nem lido pelo destinatário é uma linha ténue. Sobretudo porque na atualidade é muito simples marcar uma mensagem como não lida, ou o oposto, bem como aceder a essas mensagens em dispositivos diferentes (Fidalgo, 2019).

O Ac. do TRL, de 15/12/2009, reforça igualmente que tanto cartas e *email*s fechados e não lidos, são protegidos pelo direito constitucional da inviolabilidade da correspondência, e pelo direito à privacidade, no entanto, as cartas abertas e os *email*s já lidos, apesar de gozarem de certa proteção, só poderão ser utilizados como prova se forem obtidos de forma legítima e com respeito pelos direitos fundamentais, e pelas garantias processuais.

Para Verdelho (2004) as mensagens recebidas e não lidas devem ser equiparadas a cartas físicas fechadas, sujeitas à mesma proteção do correio físico, assim a apreensão destas mensagens deveria ocorrer mediante o art.º 179.º CPP. No caso de mensagens já lidas, o mesmo autor argumenta que, depois de abertas e armazenadas no dispositivo do destinatário, as mensagens deixam de merecer esta proteção especial. Defende ainda que após a leitura, as mensagens deveriam ser equiparadas a um documento eletrónico, sujeito ao regime de apreensão de documentos (Verdelho, 2004). No entanto, há que ter em atenção que esta doutrina é anterior à entrada em vigor da LCC.

Neves (2011) e Clemente (2022) defendem que, apesar do art.º 17.º da LCC não fazer a distinção da aplicação de regimes consoante o estado de leitura das mensagens, reconhece a existência de dois momentos diferentes. O primeiro momento é o que ocorre antes da Leitura da mensagem, que exige requisitos especiais para a sua apreensão, uma vez que a mensagem está protegida da mesma forma que uma correspondência inviolável. O segundo momento, em que a mensagem se encontra armazenada no sistema informático e já foi lida pelo destinatário, apesar de carecerem de proteção especial, não se confunde este regime com o da interceção de comunicações nem com o da apreensão de documentos, ficaria sujeito ao regime geral das apreensões, no art.º 178.º do CPP.

No mesmo sentido, Correia (2014) e Mesquita (2010) defendem que as mensagens abertas e lidas pelo destinatário se excluem do regime da apreensão de correspondência do CPP.

O Ac. do STJ n.º 10/2023 veio consolidar o entendimento de que a proteção constitucional do sigilo das comunicações eletrónicas se mantém mesmo após a leitura das mensagens. Este Ac. estabelece que, durante a fase de inquérito, a apreensão de correio eletrónico, independentemente de as mensagens estarem lidas ou não, carece sempre de autorização judicial, considerando que todas as mensagens devem ser tratadas como fechadas ou não lidas para efeitos processuais. Neste sentido, considera-se que o destinatário tem o direito de não ver a sua correspondência devassada por terceiros, independentemente do estado de leitura. Contudo, admite-se em situações de *periculum in mora,* a aplicação das medidas cautelares previstas nos termos do art.º 252.º do CPP.

O Ac. do STJ n.º 12/2024, de 20/09/2024, abordou a questão da apreensão de mensagens de correio eletrónico em processos de contraordenação, de acordo com o Regime Jurídico da Concorrência (Lei n.º 19/2012, de 8 de maio). Este Ac. estabeleceu que a competência para ordenar ou autorizar a apreensão de mensagens de correio eletrónico, independentemente de estarem abertas (lidas) ou fechadas (não lidas), pertence ao juiz de instrução. Também o Ac. do TRL, (Cf. processo n.º 184/12.5TELSB-R.L13), de 27 de junho de 2021, no mesmo sentido do anterior, estabeleceu que durante a fase de inquérito, é da competência do juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente de estarem abertas (lidas) ou fechadas (não lidas).

Na nossa perspetiva, partimos do princípio de que essa distinção não tem fundamentação jurídica, pois a violação do direito à privacidade ocorre independentemente do estado de leitura das mensagens do correio eletrónico. Apoiamos

a argumentação de Cardoso (2018) que defende que não é juridicamente correto nem adequado diferenciar o regime de apreensão com base no estado de leitura das mensagens do correio eletrónico, porque são meras indicações, que agem como filtros para o utilizador e não representam nenhuma proteção ao conteúdo da mensagem. Atendendo ao dispositivo em questão, o estado de leitura da mensagem pode variar, dependendo das definições adotadas pelo utilizador. O mesmo autor defende ainda que diferentemente do que ocorre na correspondência física, o estado de leitura das mensagens de correio eletrónico é fácil de alterar pelo utilizador. Estas mensagens podem ser arquivadas sem ser lidas, ou guardadas nos rascunhos sem serem enviadas.

3.9. A preponderância do despacho judicial prévio e o juiz enquanto a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico

A doutrina tem manifestado posições divergentes na interpretação das normas relativas à necessidade de um despacho judicial prévio, mas também sobre o papel que a reserva de juiz representa como elemento-chave na proteção dos direitos fundamentais, garantindo que os atos que afetam direitos de privacidade dos cidadãos, sejam supervisionados pela autoridade judicial. Esta garantia está contemplada no art.º 34.º n.º 4 da CRP.

No contexto da apreensão do correio eletrónico, a exigência de um despacho judicial prévio tem causado debates, uma vez que o art.º 17.º da LCC remete para o regime da apreensão da correspondência previsto no CPP, e ambos os diplomas determinam que o juiz pode autorizar ou ordenar que a apreensão se realize, mas não é explicito face ao momento em que o despacho judicial pode ser emitido o que deixa margem para dúvidas na aplicação prática deste regime. A questão persiste em saber se o despacho judicial é prévio ao ato da apreensão ou se pode ser elaborado posteriormente.

Para além disto, também se coloca a questão de saber se o juiz deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico (Clemente, 2022). Rodrigues (2009) reforça que

> em matéria processual penal, sempre que o legislador constitucional admite a abertura para a restrição de um direito, liberdade ou garantia, a mesma deve ser levada a cabo sob o estrito controlo do juiz competente e sob reserva de Lei expressa. Vigora o princípio da exclusividade jurisdicional em matéria de

> limitação de direitos fundamentais. Cabe, assim, ao juiz de instrução competente, a limitação do direito à inviolabilidade do sigilo/segredo da correspondência, sob pena de a prova, assim obtida, ser nula (art.º 179.º, n.º 1 CPP) (p. 65).

Neves (2011) defende que a aplicação do regime de apreensão de correspondência à apreensão do correio eletrónico, se deve ao facto de o juiz que ordenou ou autorizou a apreensão, ser o primeiro a tomar conhecimento do conteúdo dessas mensagens.

Verdelho (2009), pelo contrário, assume que não é necessário ser o juiz o primeiro a tomar conhecimento de todas as mensagens, uma vez que faz mais sentido que o primeiro a conhecer o conteúdo das mesmas e a fazer a primeira filtragem desses dados seja quem procede à pesquisa informática, que posteriormente encaminhará para o juiz para este decidir sobre a sua apreensão.

O Ac. de 11/01/2011, do TRL, menciona a necessidade de aplicar na totalidade o regime geral da apreensão da correspondência previsto no CPP e afirma que o primeiro a tomar conhecimento do teor das mensagens do correio eletrónico é o juiz que, posteriormente determina se autoriza ou ordena apreensão das mesmas, caso estas se considerem fundamentais para a descoberta da verdade (Cf. Processo nº 5412/08.9TDLSB-A.L1-5).

O Ac. do TRL, de 06/02/2018 (Cf. processo n.º 1950/17.0 T9LSB-A.LI-5) considera que a aplicação do regime da apreensão da correspondência se deve aplicar na sua totalidade, sem redução no seu âmbito de aplicação. Assim, exige-se que o juiz de instrução seja o primeiro a tomar conhecimento do conteúdo das mensagens de correio eletrónico. Face a isto, Cardoso (2018) refere que o art.º 17.º da LCC "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" (p. 66).

O Ac. do TRL, de 7/03/2018, alude a que, na fase de inquérito, o juiz de instrução deve exercer o seu papel na proteção dos direitos, liberdades e garantias, independentemente de a titularidade do processo ser do MP, porque estão em causa direitos fundamentais que devem ser preservados (Morim, 2022).

As diversas interpretações, fruto da inexatidão do legislador, criam algumas incoerências no sistema de tutela de direitos fundamentais no processo penal e no papel do juiz de instrução. O facto de se defender que o juiz deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens, serve para proteger os direitos fundamentais relativos à proteção da privacidade e à inviolabilidade das comunicações e o sigilo da correspondência eletrónica (Fidalgo, 2019).

No âmbito do art.º 17.º da LCC, não podem em caso algum servir como prova mensagens do correio eletrónico sem que o juiz tenha autorizado a apreensão das mesmas, a partir de um despacho judicial. No entanto, Verdelho (2009) afirma não é necessário, à luz do n.º 1 al. d) do art.º 268.º do CPP, que o juiz, seja a primeira pessoa a tomar conhecimento do conteúdo das apreensões das mensagens do correio eletrónico, pois quem procede à pesquisa informática, encaminha para o juiz apenas as mensagens selecionadas previamente como relevantes, para a investigação do caso em concreto, para o juiz posteriormente decidir sobre a sua apreensão.

Para a prova digital poder ser legível, carece de meios e conhecimentos técnicos específicos. Neste sentido, o juiz ordena à PJ para que esta proceda à abertura das mensagens do correio eletrónico e selecione as mais importantes para anexar aos autos, através de um *print.* Também pode ser solicitado a um perito de informática que se desloque ao gabinete do magistrado, para poder tomar conhecimento do conteúdo das mensagens do correio eletrónico, isto porque o juiz não tem os conhecimentos técnicos nem os equipamentos forenses essenciais para efetuar a abertura das mensagens (Ramos, 2011).

Posteriormente, o juiz pode autorizar a apreensão e junção ao processo ou pode pôr término à apreensão e entregá-la ao respetivo proprietário ou destruir o seu conteúdo (Verdelho, 2009).

Contudo, Neves (2011) afirma que esta restituição ao proprietário não é literal, uma vez que ele pode aceder na mesma às mensagens porque constam no seu sistema informático. Enquanto que a apreensão de correspondência prevista no CPP determina a remoção física da mesma da posse do destinatário, a apreensão do correio eletrónico é feita com base numa cópia da correspondência.

Verdelho (2009) salienta que a apreensão do correio eletrónico ocorre no decurso de uma busca, em que é realizada uma pesquisa informática. No entanto, durante a busca não é totalmente previsível que se encontre um computador ou outro dispositivo eletrónico, através do qual se possa aceder a mensagens no correio eletrónico relacionadas

ao crime em questão, ou que essas mensagens possam ser significativas para a investigação em curso. Desta forma, o autor aproveita para criticar o facto de ser inviável e até mesmo prejudicial ao decorrer da investigação, a indispensabilidade da autorização prévia do despacho judicial, para proceder à pesquisa informática.

Desta feita, o autor retira a conclusão de que pode existir uma apreensão cautelar das mensagens do correio eletrónico, que o juiz de instrução pode posteriormente validar, se estas mensagens forem encontradas no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático e se verificarem essenciais para o processo. Este autor também entende que a premissa requerida para uma apreensão provisória das mensagens do correio eletrónico, é existir legitimidade no acesso às mesmas, o que permite aos OPC' s que procedam à extração das mensagens de correio eletrónico para um suporte digital e o remetam convenientemente lacrado para o juiz (Verdelho, 2009). Contudo, não tem sido esse o entendimento da jurisprudência, tal como exposto nos acórdãos mencionados anteriormente.

As opiniões face a este assunto são divergentes, o Ac. do TRG, de 29-03-2011, (Cf. processo n.º 735/10.0GAPTL-A.G1) prevê que é o MP quem tem de tomar em primeira mão conhecimento das mensagens armazenas em sistemas informáticos, decidindo se estas são essenciais para a descoberta da verdade. Neste seguimento, é o MP que apreende provisoriamente as mensagens que considera relevantes e as apresenta ao juiz, para que este possa ordenar a sua apreensão, mediante um despacho judicial. Ou seja, este acórdão prevê que a apreensão provisória dos elementos convenientes ao processo é feita pelo MP, e não pelos OPC' s no decurso de uma busca (*vide* Ac. do TRG, de 29-03-2011, Processo n.º 735/10.0GAPTL-A.G1).

Relativamente à existência de um despacho judicial prévio, o n.º 1 do art.º 252.º do CPP, relativo à apreensão da correspondência, permite a posterior convalidação judicial, confirmada pelo n.º 3 do mesmo artigo, numa perspetiva de suspensão da correspondência pelos órgãos de polícia criminal, até decisão judicial. Caso o juiz não autorize a apreensão, no prazo de quarenta e oito horas, a correspondência é remetida ao destinatário, ou destruída. Para o caso de encomendas ou valores fechados, pelo risco da informação se perder ou pelo *periculum in mora* da investigação, os OPC's informam prontamente o juiz para que este autorize a sua abertura imediata (Verdelho, 2009).

Clemente, (2022) defende que o legislador não foi preciso na definição do momento em que o despacho prévio deve ser emitido, no entanto, outra interpretação distinta não parece razoável, pois iria recair sobre o juiz a necessidade de analisar

individualmente todas as mensagens de correio eletrónico de todos os dispositivos para se puder proceder à apreensão, o que não seria de todo sustentável.

Apesar da opinião anteriormente defendida por Clemente (2022), a jurisprudência tem tido um entendimento divergente, como vemos no Ac. do STJ nº 10/2023 (Diário da República, 1 de março de 2023), que estabelece que, na fase de inquérito compete ao juiz de instrução ordenar e autorizar a apreensão de mensagens de correio eletrónico, mesmo que as mensagens já tenham sido abertas e lidas pelo destinatário, a sua apreensão sem autorização judicial prévia é ilegal, considerando-as sempre como "fechadas" para efeitos processuais, argumentando que merecem ambas a mesma proteção constitucional. Este Ac. refere que "independente de a correspondência ter sido ou não aberta ou ter sido ou não lida, a pessoa a quem é dirigida tem sempre o direito de não ver essa correspondência devassada por terceiros". No entanto, o mesmo Ac. reforça que se admite para situações de *periculum in mora,* a medida cautelar prevista no art.º 252.º do CPP.

Correia (2014) defende que, de acordo com o Tribunal Constitucional Federal Alemão, a ingerência em sistemas informáticos de terceiros para acesso a dados, só seria admissível mediante um despacho judicial prévio. Em Portugal os tribunais têm compreendido que o único despacho que pode autorizar a apreensão do correio eletrónico é o despacho emitido pelo juiz, e de outro modo a prova culminaria numa nulidade (art.º 120.º n.º 2 CPP). O primeiro a aceder ao conteúdo das mensagens do correio eletrónico deve ser o JIC, sendo um ato da sua exclusiva competência com base no art.º 268.º, n.º 1 do CPP, caso contrário a prova é proibida (art.º 126.º n.º 3 do CPP) pois acaba por ser uma intromissão ilegítima na vida privada e na correspondência, (Cf. o n.º 8 do art.º 32.º e o n.º 4 do Art.º 34.º) (Fidalgo, 2019).

A incoerência apontada relativamente aos papéis do MP e dos OPC's, entre o regime da apreensão de correio eletrónico e o regime de interceção de comunicações, centra-se no carácter acusatório do processo penal, em que o MP lidera a investigação e a recolha das provas. O ponto de controvérsia surge da potencial sobreposição das funções do juiz às exercidas pelo MP ao longo do inquérito (Fidalgo, 2019). O MP e os OPC's podem fazer uma recolha técnica em determinados casos previstos no correio eletrónico, de forma provisória, mas o mesmo não é admissível nem aplicável às escutas telefónicas, neste último meio de obtenção de prova, o momento de intervenção judicial é inquestionável, já na apreensão de correio eletrónico acaba por ser ambíguo.

Durante o inquérito, cabe ao MP realizar a apreensão ou delegar esta função nos OPC's, no entanto, a apreensão de mensagens de correio eletrónico implica a realização de cópias das provas, sendo um processo que requere conhecimentos técnicos e ferramentas informáticas que os magistrados não possuem. A iniciativa para dar início à apreensão não se pode confundir com a decisão judicial de autorizar a apreensão. O juiz de instrução não define que mensagens devem ser ou não apreendidas e ao mesmo tempo, o MP também não pode requerer a apreensão de mensagens que desconhece, já que lhe cabe decidir sobre a prova relevante e indispensável para a investigação (Cardoso, 2018).

Nunes (2021) reforça que a Lei, neste caso, não pode ser interpretada de forma literal, primeiro porque desde logo o objeto da apreensão é distinto, as dificuldades operacionais e técnicas associadas à apreensão do correio eletrónico não permitem que a apreensão seja apenas levada a cabo após despacho judicial para o efeito. Com base nisto, o mesmo autor defende que é praticamente impossível o juiz ser o primeiro a tomar conhecimento do conteúdo das mensagens do correio eletrónico, embora seja efetivamente este a autorizar a apreensão e a decidir sobre a sua junção ao processo.

No caso de Interceção de comunicações do art.º 18.º da LCC, que manda aplicar o previsto nos art.º(s) 187.º, 188.º, 190.º do CPP, em tudo o que não for contrariado pela mesma Lei. O art.º 188.º do CPP concede aos OPC's a prerrogativa de serem os primeiros a aceder ao conteúdo das comunicações, se estiverem previamente autorizados pelo juiz para o fazer. Se tal ocorresse na apreensão do correio eletrónico, entendia-se uma maior celeridade e agilização nas investigações e a concentração das atenções somente no conteúdo das provas relevantes (Fidalgo, 2019).

Compreendemos o benefício da celeridade na investigação invocado por Fidalgo (2019), no entanto, a nossa posição, em consonância com Ac. do STJ n.º 10/2023, de 10 de novembro, é que deve ser o juiz de instrução o primeiro a tomar conhecimento do conteúdo das mensagens, para não se subverter o princípio da reserva de juiz consagrado no artigo 34.º, n.º 4 da CRP, e garantir a existência de uma proteção efetiva dos direitos fundamentais, bem como a legalidade e validade da prova. À semelhança do exposto por este Ac., compreendemos que o visado tem o direito de não ver a sua correspondência devassada por terceiros e, como tal, deve ser o juiz o primeiro a tomar conhecimento do conteúdo das mensagens de correio eletrónico, independentemente do estado de leitura das mesmas. Para além disto, entendemos que deve-se conservar conforme estipulado anteriormente, as situações de *periculum in mora* da investigação.

Ainda assim concordamos com Cardoso (2018) quando este autor defende que não é porque o juiz é o primeiro a tomar conhecimento do conteúdo das mensagens de correio eletrónico, que o MP não o venha a fazer posteriormente. Isto vem da lógica que caso o juiz decida não juntar os elementos de prova ao processo, o MP tem o direito de recorrer desta decisão, e não pode fundamentar o recurso de uma decisão sobre elementos de prova que desconhece.

Capítulo IV. Conhecimentos fortuitos e sua admissibilidade

4.1. Distinção entre conhecimentos fortuitos e conhecimentos de investigação

A introdução da temática dos conhecimentos fortuitos no ordenamento jurídico português, surge pela primeira vez na Lei n.º 48/2007, 29 de agosto, na 15ª alteração ao CPP, que consagrou no art.º 187.º, n.º 7 e 8 esta matéria, no âmbito das escutas telefónicas. Antes desta previsão legislativa, a doutrina já reconhecia a possibilidade da admissibilidade dos conhecimentos fortuitos como meio de obtenção de prova. Tal necessidade justificou-se pela frequente obtenção de conhecimentos relativos a terceiros, ou a outros crimes, que não são abrangidos pelo despacho do JIC, que autoriza a realização da diligência em questão (muito frequente na obtenção de prova por escutas telefónicas). Em sentido amplo, os conhecimentos fortuitos subdividem-se em conhecimentos fortuitos *stricto sensu* e conhecimentos de investigação (Morim, 2022). Vamos dedicar este capítulo a aprofundar a definição de conhecimentos fortuitos, bem como, a delimitação das suas fronteiras.

Os conhecimentos de investigação surgem com naturalidade no processo, são decorrentes dos factos que estão a ser investigados, a partir dos quais é emitido o despacho judicial para o efeito, dedicam-se a construir o objeto do processo. A legitimidade para a sua utilização é consequência do despacho de autorização judicial, como tal, estes conhecimentos já não são suscetíveis de tantas restrições para a sua incorporação no processo, pois dizem respeito ao "mesmo pedaço de vida" da investigação em curso (Neves, 2012, p. 70).

Os conhecimentos da investigação estão em concurso ideal e aparente com o crime em questão. Os crimes que são descobertos posteriormente não se tratam em todos os casos de conhecimentos fortuitos, fazem parte dos acontecimentos desencadeados pelo crime investigado e são oportunamente submetidos a julgamento, fazendo parte de conhecimentos complementares ao processo (Andrade, 1992).

A admissibilidade dos conhecimentos de investigação não carece de uma nova autorização judicial, porque se constituem como o objeto da investigação e como tal, existe flexibilidade nos dados e informações que são transportados para o processo. Ainda assim, os conhecimentos de investigação, apesar de darem origem a mais elementos de prova, têm uma estreita conexão com o objeto da investigação (Morim, 2022).

Já os conhecimentos fortuitos, podem dar origem a processos diferentes do original, por terem dados e informações que não se relacionam com o objeto do processo nem com o despacho que legitimou a investigação. A valoração dos conhecimentos fortuitos trata-se de aproveitar os dados relativos a outros crimes, em contexto de processos diversos, recolhidos na investigação legitimamente executada (Morim, 2022).

Os conhecimentos fortuitos encontram-se plasmados no art.º 187.º n.º 7 do CPP. A distinção entre estes e os conhecimentos de investigação tem sido mantida na jurisprudência, como demonstram os acórdãos do STJ, de 18/03/2010 (Processo n.º 110/06.0TTCBR.C1.S1) e 29/04/2010 (Processo n.º 128/05.0JDLSB-A.S1). Os conhecimentos fortuitos no âmbito da realização das escutas telefónicas, surgem através daquilo que é captado pelas autoridades durante as conversações, não é o produto de acontecimentos que estão a ser investigados, antes aparecem de forma inesperada. Uma vez que estes conhecimentos não resultam dos crimes vertidos no despacho judicial, a sua utilização está sujeita a exigências e restrições para a sua admissibilidade (Neves, 2012).

Andrade (1992) definiu os conhecimentos fortuitos como acontecimentos que "não se reportam ao crime cuja investigação legitimou a sua realização" (p. 304). Se estes conhecimentos não dizem respeito às infrações previstas nos crimes de catálogo, previstos no art.º 187, n.º 1 do CPP, a dificuldade na sua admissibilidade é maior. Os conhecimentos fortuitos não convergem com os factos do processo, são crimes descobertos à posteriori, com o decorrer da investigação, *hoc sensu*, não se traduzem conceptualmente no objeto do processo.

Relativamente às escutas telefónicas, Andrade (1992) salienta que a única limitação face à valoração da prova, é quando estas remetem para proibições de produção de prova, em que, neste último ato exista alguma violação da Lei. O mesmo autor reconhece que existe uma determinada urgência em sinalizar a separação entre os conhecimentos da investigação e os conhecimentos fortuitos, mas ao mesmo tempo há também uma denotada dificuldade em fazê-lo, pois existem sempre conexões entre eles, o que torna esta distinção muito complexa.

Existe também um critério de ponderação da proporcionalidade da valoração das provas que se regem pelo regime das escutas telefónicas, entre a ponderação de vários valores, como a gravidade da infração ou o grau de suspeita que vale para a autorização da escuta telefónica. Os conhecimentos fortuitos impendem sobre a afetação de direitos relativos à intromissão na esfera da vida privada dos indivíduos e alguns autores argumentam com a ideia de estado de necessidade da investigação, como fundamento que

legitima a admissibilidade de provas que comprometam os direitos de privacidade dos cidadãos (Andrade, 1992).

O n.º 1 do art.º 179.º do CPP, respeitante ao regime de apreensão da correspondência, contém os requisitos cumulativos respeitantes a um regime de catálogo análogo ao expressamente regulamentado para o regime das escutas telefónicas, o que significa que a admissibilidade da apreensão da correspondência está condicionada ao cumprimento destes requisitos, que impõem limites rigorosos à obtenção e utilização deste meio de prova. Todos os crimes que não estejam em conexão com este regime de catálogo, estão vinculados ao princípio da proibição de valoração de conhecimentos fortuitos (Andrade, 1992). Aguilar (2016) argumenta que os critérios de conexão com os crimes investigados servem como parâmetro que separa os conhecimentos de investigação dos conhecimentos fortuitos. Concordamos que esta delimitação é essencial para garantir a proteção dos direitos fundamentais dos cidadãos, assegurar a legalidade da prova recolhida e evitar qualquer utilização abusiva da interceção de comunicações. Sem este critério, poderia correr-se o risco de alargar indevidamente o âmbito da investigação criminal, comprometendo os princípios fundamentais do Estado de direito.

O art.º 24.º n.º 1 do CP, respeitante à conexão de processos, estabelece critérios objetivos para decidir se factos descobertos no decurso de uma investigação se relacionam estreitamente com o crime a ser investigado. Se essa conexão se verificar, tais factos poderão ser usados no mesmo processo, caso contrário, são conhecimentos fortuitos. Esta perspetiva é adotada tanto em Espanha como em Itália, a utilização da prova depende da conexão dos factos com o crime investigado. Em Espanha, caso não se verifique essa relação, os factos servem apenas como um alerta para uma investigação futura. Já em Itália, o CPP impõe limites ao uso de escutas telefónicas, esta restrição aplica-se quando são descobertos novos factos que não podem ter o mesmo tratamento que os factos decorrentes da investigação (Neves, 2012).

A doutrina tem proposto diferentes soluções relativamente à admissibilidade dos conhecimentos fortuitos, nomeadamente, Neves (2012) elenca quatro interpretações principais neste âmbito. A primeira interpretação (associada a Germano Marques da Silva) entende que basta que o meio de comunicação usado conste no despacho judicial, sendo irrelevante a identidade da pessoa visada. No entanto, esta visão é criticada por ignorar os critérios estabelecidos pelo art.º 187.º n.º 4 do CPP. A segunda interpretação admite apenas a valoração dos conhecimentos fortuitos apenas quando a pessoa escutada for uma das abrangidas pelo despacho judicial, relativamente ao crime investigado. Esta

segunda hipótese é mais restritiva e o critério preponderante é apenas a identidade da pessoa que está a ser ouvida, pode eventualmente excluir situações em que a prova seria relevante e teria sido recolhida de forma válida. O terceiro critério e aquele que é defendido por Neves (2012) entende que os conhecimentos fortuitos podem ser valorados mesmo que respeitem a crimes diferentes daqueles que motivaram a escuta, desde que o visado pela interceção de comunicações conste no n. º4 do art.º 187.º do CPP, em relação ao novo crime descoberto. Esta admissibilidade é aferida à posteriori, verificando-se com base nos mesmos requisitos legais, se a escuta seria legítima para o novo objeto. Por fim, a quarta interpretação sugere uma leitura mais abrangente dos critérios legais, que admite a valoração dos conhecimentos fortuitos sempre que a pessoa escutada se enquadre no n.º 4 do art.º 187.º do CPP, relativamente ao crime investigado, ou em relação ao crime descoberto fortuitamente. Contudo, esta interpretação acaba por enfraquecer o papel da autorização judicial e acaba por não fornecer um critério equilibrado nem em termos de direitos fundamentais nem na eficácia da investigação (Neves, 2012).

A nossa perspetiva coaduna-se com o entendimento do próprio autor, ao defender que a terceira interpretação é a solução mais equilibrada e a que concilia melhor a proteção dos direitos fundamentais com a eficácia da investigação.

Em suma, a distinção entre os conhecimentos fortuitos e os conhecimentos de investigação pode gerar algumas contradições, porque ambos abrangem factos que podem ir para além do escopo da investigação. No entanto, os conhecimentos de investigação fazem parte do desenvolvimento da fase do inquérito, ao passo que, os conhecimentos fortuitos são factos encontrados de forma inesperada. A figura dos conhecimentos fortuitos foi pensada para o regime das escutas telefónicas, sempre que eram captados ocasionalmente durante a diligência, elementos que não se relacionavam com o crime investigado, nem com o despacho que originou tal investigação (Reis, 2023).

4.2. A admissibilidade dos conhecimentos fortuitos

A admissibilidade dos conhecimentos fortuitos é uma questão central no direito processual penal, e para entender a sua aplicação, é importante compreender que existem requisitos essenciais a ter em conta.

A doutrina Alemã influenciou significativamente as soluções adotadas por Portugal no que diz respeito à admissibilidade e ao regime processual dos conhecimentos fortuitos. Em 1973, o Tribunal Estadual Superior Hanseático determinou que a

legitimidade das escutas telefónicas que originaram os conhecimentos fortuitos era suficiente para que estes fossem utilizados num segundo processo. No entanto, em 1976, o Tribunal Federal Alemão impôs mais restrições à sua admissibilidade, exigindo que os factos obtidos envolvessem algum tipo de ligação com um crime previsto num catálogo específico. Além disso, a utilização desses conhecimentos deveria respeitar o princípio da proporcionalidade. Em 1978, o Tribunal Federal Alemão avançou com uma exigência de conexão estreita entre os factos descobertos fortuitamente e o crime que justificou a investigação, especialmente em casos de terrorismo e criminalidade violenta (Andrade, 1992).

No âmbito dos conhecimentos fortuitos, no ordenamento jurídico norte-americano, a *plain view doctrine* tem sido amplamente estudada como uma exceção à regra e do cumprimento dos trâmites legais. A lógica que fundamenta esta tese baseia-se na ideia de que o investigador perceciona, no decurso de uma busca legítima, elementos de prova que, apesar de não estarem abrangidos pelo despacho judicial, são ilícitos e não podem ser ignorados. Com base nesta perspetiva, se a busca tiver sido legitimamente autorizada e realizada, se um facto ilegal é percebido a olho nu, a sua utilização no processo é justificada. Esta tese decorre do princípio da *reasonableness,* que analisa se houve uma violação da Quarta Emenda[8], quer na emissão do mandado como na forma como se conduziu a busca. Desta forma, provas que extravasem o objeto do processo são submetidas a este princípio. Esta doutrina teve a sua aplicação no ambiente físico, e cada vez mais têm surgido debates sobre a aplicação desta doutrina ao ambiente digital (Reis, 2023)

Sob esta possibilidade, a *plain view doctrine* tem sido interpretada à luz de três abordagens distintas no contexto digital, a primeira é a adaptação desta doutrina ao meio digital, com a aceitação da visualização enquanto critério de legitimação; a segunda é a necessidade de medidas corretivas e do critério de inadvertência, que exige limites claros e um controlo judicial adicional e, por último; a rejeição total da aplicação desta doutrina ao ambiente digital (Reis, 2023).

Na primeira abordagem, alguma jurisprudência defende que os investigadores podem abrir os arquivos e verificar o seu conteúdo, desde que esses arquivos sejam diretamente visíveis e acessíveis no decurso da diligência autorizada. Argumenta-se que,

[8] De acordo com Reis (2023) a Quarta Emenda está designada na constituição dos EUA e protege os cidadãos contra buscas e apreensões indiscriminadas por parte do Estado. Com base nesta doutrina, cada investigação carece de bases legais sólidas ou um mandado judicial bem fundamentado. *A plain view doctrine* vem atuar como uma garantia da efetividade da Quarta Emenda.

no ambiente digital, a visualização é, muitas vezes, uma forma de confirmar a natureza ilícita dos elementos probatórios (Reis, 2023).

Na segunda abordagem a jurisprudência considera que se os agentes tentarem procurar elementos de prova que extravasem o objeto do despacho judicial é lhes exigido que requeiram um novo mandado judicial para proceder à apreensão de elementos de prova relativos esses novos elementos de prova, que configuram crimes diversos. O objetivo é impedir que provas relativas a outros crimes, sejam usadas indiscriminadamente, sem o devido controlo judicial (Reis, 2023).

A última abordagem sustenta que, provas relativas a crimes que ultrapassam a investigação em curso e encontradas fortuitamente devem ser recusadas de forma absoluta. Esta perspetiva parte do princípio de que, dada a imensidão de dados e informações disponíveis no ambiente digital, permitir a apreensão de provas fortuitas pode configurar práticas abusivas e investigações indiscriminadas, favorecendo aplicações incompatíveis com os princípios da legalidade, da necessidade e da proporcionalidade (Reis, 2023).

Em Portugal, a utilização de conhecimentos fortuitos é regulamentada no art.º 187.º, n.º 1 do CPP, que trata da admissibilidade das escutas telefónicas, onde se lê, crimes "puníveis com pena de prisão superior, no seu máximo a 3 anos", "relativos ao tráfico de estupefacientes", "de detenção de arma proibida e de tráfico de armas", "de contrabando", "de injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone", "de ameaça com prática de crime ou de abuso e simulação de sinais de perigo" e "de evasão, quando o arguido haja sido condenado por algum dos crimes". O n.º 7 do mesmo artigo, permite que as comunicações legalmente intercetadas num processo, possam ser utilizadas, embora tal se verifique apenas quando for fundamental para provar os factos do crime a ser investigado. O uso desta prova no âmbito de outro processo não pode ser arbitrário e só pode ser usada quando não existirem outros meios de obtenção de prova que se revelem eficazes, de modo a garantir o respeito pelos princípios da necessidade e da subsidiariedade (Morim, 2022).

Segundo Andrade (2009), os conhecimentos fortuitos obtidos como resultado das escutas telefónicas, só devem ser admissíveis se houver legitimidade para autorizar as escutas telefónicas desde o início. O autor recorre ao "princípio da intromissão sucedânea hipotética" (pp. 173-174). Quer isto dizer que, a prova só pode ser valorada se, hipoteticamente, a escuta tivesse sido aproveitada para a investigação do novo crime.

A utilização dos conhecimentos fortuitos num processo distinto daquele em que foram recolhidos, depende de autorização judicial, onde o juiz deve analisar se está a ser dado cumprimento aos requisitos legais. Nos termos do n.º 8 do art.º 187.º do CPP, sempre que, no decurso de uma interceção de comunicações, se obtiverem elementos que constituam a prática de um crime diferente do inicialmente investigado, esses conhecimentos só podem ser utilizados se tal for previamente autorizado por um juiz, (desde que estejam reunidos os pressupostos legais exigidos). Não está explicito nas normas do art.º 187 n.º 8 do CPP, qual deve ser o juiz competente para tomar essa decisão, o que tem suscitado divergências doutrinárias e uma difícil aplicação prática. Desta forma, a competência do juiz varia conforme a fase processual em que essa autorização é requerida, i.e., na fase de instrução o MP solicita ao JIC e na fase de julgamento, ao juiz de julgamento (Morim, 2022).

A doutrina defende que deve existir uma necessidade de investigação que dê motivo à realização das escutas telefónicas, à luz dos art.º(s) 26.º e 32.º da CRP, sendo essencial garantir que não haja nenhuma utilização abusiva das provas recolhidas, e o mesmo é adaptado às diligências efetuadas em ambiente digital. O Ac. do STJ, de 23/10/2002, concordou com a posição defendida por Andrade (1992). A utilização dos conhecimentos fortuitos só é permitida se forem cumpridos certos requisitos. Entre eles, exige-se que as escutas que deram origem aos conhecimentos, tenham cumprido rigorosamente as normas previstas no art.º 187.º, n.º 1 do CPP, o crime em causa deve também estar contemplado no catálogo legal. Outro requisito essencial é que as informações recolhidas devem ter um peso significativo na busca pela verdade e na produção de prova para o processo. Deve ser garantido ao arguido o direito ao contraditório, permitindo-lhe contestar o uso dos conhecimentos fortuitos (Morim, 2022).

A doutrina tem-se mantido alheia relativamente à adaptação da admissibilidade dos conhecimentos fortuitos para meios de obtenção de prova divergentes das escutas telefónicas. Esta decisão foi propositadamente tida em conta pelo legislador, isto porque, no decurso de uma investigação, se o meio de obtenção de prova usado foi legítimo e concordante com o despacho que o determinou, os elementos probatórios recolhidos também o serão (Reis, 2023).

Valente (2004) assume que os meios de obtenção de prova podem ser operacionalizados enquanto medidas cautelares e de polícia, perante o estado de necessidade da investigação, sob condição de uma posterior validação pela AJ competente. Este autor menciona que os conhecimentos fortuitos estão interligados com

os crimes de catálogo que dependem eventualmente do uso de métodos ocultos de obtenção de prova.

Quer a jurisprudência referida anteriormente, quer o defendido por Andrade (2009), defendem que deve existir uma admissibilidade geral para a apreensão e valoração dos conhecimentos fortuitos, mesmo que não se relacionem com a investigação em curso. A argumentação para esta posição, reside no facto de os conhecimentos fortuitos decorrentes de outros métodos de obtenção de prova não se equipararem à problemática levantada pelas escutas telefónicas. A título de exemplo, para a realização de buscas (Cf. art.º 174.º, 176.º e 177.º do CPP) existem também requisitos próprios que legitimam este meio de obtenção de prova, nomeadamente no âmbito das buscas domiciliárias. No entanto, não existe um catálogo de crimes que preveja concretamente nesses casos a realização de buscas, mas tal não significa que por não estarem previstos, possam ser realizadas (Reis, 2023).

No nosso entendimento, a admissibilidade dos conhecimentos fortuitos, exige uma análise casuística criteriosa. Neste sentido, sustentamos que devem ser ponderados diversos critérios, nomeadamente o contexto específico em que os conhecimentos foram adquiridos, verificando se a diligência foi realizada dentro dos parâmetros legais e conduzida de forma legítima. Há que avaliar o grau de suspeita existente e a gravidade da infração (relativamente ao enquadramento dos factos nos crimes previstos no catálogo do n.º 1 do art.º 187.º do CPP).

Adicionalmente, defendemos que, importa avaliar se foram cumpridos os requisitos formais, inerentes aos meios de obtenção da prova, bem como o respeito escrupuloso pelo despacho que determinou a investigação. Afiançamos que a admissibilidade destes conhecimentos deve sempre resultar de uma ponderação de valores, garantindo que a descoberta da verdade material não se traduz numa violação desproporcional de direitos, liberdades e garantias. Tem que ser analisada a necessidade da prova para o esclarecimento dos factos em questão. Assim, na nossa apreciação, a valoração dos conhecimentos fortuitos deve estar sujeita ao princípio da proporcionalidade, assegurando que a sua valoração tem em vista a necessidade e adequação da prova aos fins da investigação criminal, sem comprometer os limites impostos num Estado de Direito Democrático.

4.3. A admissibilidade dos conhecimentos fortuitos no correio eletrónico

Ao contrário do que sucede no regime das escutas telefónicas, a legislação não prevê expressamente, no regime de apreensão de mensagens de correio eletrónico e registos de comunicações de natureza semelhante, qualquer referência específica quanto à valoração dos conhecimentos fortuitos (Morim, 2022). Importa, por isso, determinar, como foco do presente estudo, se as mensagens do correio eletrónico apreendidas no âmbito de um processo anterior podem ser utilizadas como meio de prova num processo distinto.

Face a isto, a doutrina tem-se debruçado sobre a aplicação analógica do n.º 8 do art.º 187.º do CPP, ao correio eletrónico. Valente (2004) defende que se deve adotar a mesma lógica que rege a admissibilidade dos conhecimentos fortuitos no âmbito das escutas telefónicas, ao correio eletrónico.

Fidalgo (2019) considera que a inexistência legal de um regime geral de conhecimentos fortuitos, não impede a admissibilidade do seu uso em outro processo distinto. Afirma a mesma autora que deve ser feita uma interpretação normativa, como já era prática antes da previsão legal da norma inserida em 2007.

Cardoso (2019) concorda com a posição dos autores referidos anteriormente e afirma que se os meios de obtenção de prova, que deram origem a esses conhecimentos, tiverem sido válidos, (entenda-se o acesso legítimo a um sistema informático, com base no art.º 11 n.º 1 da LCC), e se não existir uma limitação relativamente ao meio de obtenção de prova ou ao objeto do processo, a utilização dos conhecimentos fortuitos deve ser aplicada sem restrições, sempre que respeite os limites legais.

Um exemplo prático desta problemática encontra-se no Ac. do TRL, de 11/07/2019, no qual foi apreciada a admissibilidade de mensagens de correio eletrónico apreendidas no âmbito de um processo, pretendendo o MP o seu uso num processo distinto. Neste sentido, o MP solicitou ao JIC uma autorização para realizar uma nova pesquisa informática sobre as mensagens do correio eletrónico já apreendidas, o que levou o JIC a declarar a nulidade do despacho judicial anterior, argumentando que era da sua competência conceder tal autorização, uma vez que era o juiz competente no processo onde se pretendia usar a prova. O MP recorreu desta decisão, porque defendia que quem poderia conceder essa autorização eram os juízes de instrução responsáveis pelo processo de origem (Morim, 2022).

O Ac. do TRL decidiu que o juiz competente no segundo processo não tinha competência para reapreciar a legalidade de uma prova que já tinha sido validada no processo original. Foi também determinado que a nova pesquisa que o MP solicitou não se enquadrava no conceito de conhecimento fortuito. Esta decisão gerou debate, porque a realização de uma pesquisa informática, pressupõe que se desconhece o seu conteúdo, e se este for intencionalmente averiguado, não se pode considerar que as provas tenham surgido fortuitamente no processo. No entanto, o Ac. do TRL acabou por reconhecer que mensagens do correio eletrónico, que já foram apreendidas num primeiro processo, podem ser usadas como meio de prova num segundo processo, se tiverem sido devidamente validadas e se tiverem sido respeitados os limites legalmente estabelecidos (Morim, 2022).

A jurisprudência tem vindo a permitir a aplicação do regime que determina a admissibilidade dos conhecimentos fortuitos nas escutas telefónicas ao correio eletrónico, no entanto, os requisitos para a sua valoração não são integralmente os mesmos, atendendo a que a afetação dos bens jurídicos em causa diverge. Conclui-se que as mensagens do correio eletrónico apreendidas no decorrer de um processo podem ser usadas no âmbito de um processo distinto, se forem respeitados os princípios da legalidade, proporcionalidade, reserva de juiz e sempre que a prova tenha sido obtida com base nos limites estabelecidos pelo ordenamento jurídico (Fidalgo, 2019).

Compreendemos que, atualmente, não existe um regime jurídico específico, que determine a admissibilidade dos conhecimentos fortuitos no correio eletrónico, nem mesmo um catálogo de crimes neste regime, que delimite em que situações pode ser valorada uma prova que não esteja diretamente relacionada com o objeto da investigação. Partilhamos da mesma visão de Fidalgo (2019) e Cardoso (2019) no sentido em que se a prova for obtida legitimamente, respeitando integralmente o conteúdo do despacho que determinou a investigação, e cumprindo todos os requisitos formais no que respeita ao meio de obtenção de prova, os conhecimentos fortuitos devem ser tendencialmente admissíveis. Contudo, é indispensável que a apreensão da qual resultam os conhecimentos fortuitos, seja previamente validada por despacho judicialmente fundamentado, onde se demonstre a necessidade de investigação criminal em curso.

Porém, não podemos desconsiderar que esta admissibilidade deve sempre resultar de uma ponderação criteriosa entre valores jurídicos em conflito, assegurando que a busca pela verdade material não implique uma violação injustificada e desproporcional dos direitos, liberdades e garantias do visado ou de terceiros. Assim,

concluímos que a valoração dos conhecimentos fortuitos, deve estar subordinada ao princípio da proporcionalidade, garantindo um equilíbrio adequado entre a eficácia da investigação criminal e a proteção dos direitos fundamentais. Apoiamos a decisão do Ac. do TRL, de 11/07/2019, em que cabe ao juiz de instrução competente no processo original, decidir sobre a possibilidade da sua utilização num processo subsequente. Desta forma, em conformidade com o princípio da reserva de juiz, é assegurada a coerência e a continuidade na apreciação e legalidade da prova (conforme o princípio da fixação de competências).

4.4. O perigo das *phishing expeditions* e os critérios de pesquisa informática

Assumindo que para a investigação de um crime é necessário que existam fundadas suspeitas que legitimem o uso de métodos de obtenção de prova, não parece razoável que qualquer tipo de prova possa ser admissível (Reis, 2023). A realização de diligências processuais tem um fim claro, que jamais pode ser confundido com a obtenção de prova indiscriminadamente, estando as mesmas sujeitas a princípios constitucionais, já previamente abordados em capítulos anteriores.

Neste contexto, surge a problemática das chamadas *phishing expeditions.* Um despacho judicial que legitima uma investigação, não deve ser interpretado como uma autorização irrestrita para que o investigador, munido dessa legitimidade, proceda indiscriminadamente à averiguação de toda e qualquer prova. Importa destacar que nem sempre o alvo da diligência é o arguido, apesar de o ser na maioria dos casos. Ainda assim, a recolha de prova acaba por afetar este sujeito processual, porque é face a ele que a diligência é dirigida. Razão pela qual, é essencial garantir a proteção dos direitos do arguido no processo, concretamente o princípio da presunção da inocência, vertido no art.º 32.º n.º 2 da CRP. Tal princípio consagra que ao longo de todo o processo penal, o arguido tem direito a ser tratado com base no princípio *in dubio pro reo*, devendo este ser sempre arrogado como inocente até ao trânsito em julgado da sentença de condenação (Reis, 2023). Dias (2004) considera, este, um "direito subjetivo", reconhecido na jurisprudência (p. 122).

A positivação deste direito protege e impede o cometimento de abusos, a sua aplicação não se limita ao tratamento que o arguido deve receber no decorrer do processo, mas estende-se também à obtenção e admissibilidade da prova. Apesar da recolha de prova ser um sacrifício necessário que permite a descoberta da verdade material, devem

ser estabelecidas consequências para evitar qualquer ingerência indevida nos direitos, liberdades e garantias dos visados. A obtenção de prova deve respeitar rigorosamente os limites estabelecidos pelo despacho judicial que ordenou a diligência. Apesar disto, o entendimento de Reis (2023) não coincide com rejeitar todos os conhecimentos fortuitos obtidos na investigação, pelo contrário, a autora afirma que devem ser admissíveis os conhecimentos que forem fruto de um cumprimento exigente de todos os requisitos contantes no despacho que permitiu a investigação (Reis, 2023).

O Ac. do TRL, de 13/09/2007, que revogou a decisão proferida pelo Tribunal de 1ª instância, determinou que, no decorrer de uma busca, cuja recolha de elementos probatórios não apresenta especificidades, todas as provas podem ser utilizadas no processo. O MP salientou, no caso em questão, que apesar dos elementos probatórios apreendidos não se relacionarem à investigação, os conhecimentos fortuitos originários dessa busca são admissíveis, por razões de economia processual, da não adulteração da prova e porque a busca foi realizada de acordo com os parâmetros legais da autorização judicial para o efeito (Reis, 2023).

O referido Ac. é uma demonstração de uma abordagem jurisprudencial que procura equilibrar os fins da investigação criminal com a tutela dos direitos fundamentais dos visados. Este Ac. reflete que a recolha de elementos probatórios que excedam o objeto da investigação podem ser válidos, desde que a diligência tenha sido realizada de acordo com os parâmetros legais definidos. A perspetiva do MP neste Ac. demonstra especial preocupação com a integridade da prova, uma vez que evita a inutilização de elementos probatórios descobertos, desde que não vão para além dos limites legais da diligência.

Esta realidade, embora observada no ordenamento jurídico português, encontra paralelo noutras jurisdições, como é o caso dos EUA, que no ano de 1994, com a intenção de orientar os procedimentos adotados pelos OPC's nas buscas e apreensões no ambiente digital durante as investigações, o departamento de justiça publicou as *Federal Guidelines for Searching and Seizing Computers* (Cf. *Federal Guidelines for Searching and Seizing Computers*, 1994).

Estas diretrizes foram posteriormente atualizadas e revistas em 2009, para *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* As diretrizes em causa, eram relativas a pesquisas informáticas em discos rígidos, e nos restantes sistemas e equipamentos informáticos, onde se inclui o correio eletrónico. O principal objetivo destas diretrizes consistia em impedir as *phishing expeditions,* e limitava a pesquisa ao estipulado pelo mandado judicial, restringindo o seu

objeto aos crimes investigados. Assim, uma pesquisa com base em palavras-chave específicas relativas à investigação, iria limitar a quantidade de dados a que os investigadores tinham acesso, diminuía consequentemente a probabilidade de se depararem com conhecimentos fortuitos, e reduzia a afetação da privacidade dos visados (Cf. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009).

Os documentos que eram sinalizados pela pesquisa, posteriormente eram copiados para suporte digital e apreendidos, para serem presentes ao juiz. Este tipo de pesquisa informática garante proporcionalidade e garantias contra eventuais abusos. O objetivo desta pesquisa delimitada de forma rigorosa, é limitar o objeto da pesquisa de dados, ficheiros e documentos informáticos (Mendes, 2021).

> Tal só é viável, porém, se as autoridades públicas tiverem de antemão uma perceção rigorosa das evidências de que estão à procura, uma espécie de evidência conclusiva vulgo, a *smoking gun evidence*[9] do delito sob investigação, que, por exemplo, lhes tenha sido revelada com exatidão por um denunciante. Nestes casos, o procedimento de utilização de palavras-chave é preferível para todos (Mendes, 2021, p. 239).

Se não for possível realizar esta pesquisa por palavras-chave no momento em que ocorre a busca, faz-se uma cópia integral do servidor. No entanto, as diretrizes de 2009 revelam a diferença entre uma cópia integral dos ficheiros e uma cópia de ficheiros individuais. Esta última, permite que não se ultrapasse o objeto da investigação. A pesquisa por palavras-chave consiste numa seleção pormenorizada e célere, mas não se insere em nenhum contexto, são palavras vagas e podem dar origem a designações erróneas, consequentemente, os dados obtidos podem ir para além do objeto do despacho judicial. Um exemplo em que foi utilizada uma pesquisa informática por palavras-chave em computadores, foi o caso Sérvulo & Associados[10]. (Mendes, 2021).

[9] Mendes (2021) utiliza a expressão *smoking gun evidence,* que representa uma metáfora jurídica qualificada como uma prova inequívoca, que não gera qualquer dúvida na sua interpretação. Afirmando que só assim as autoridades poderiam saber as provas que procuravam no âmbito da investigação e nesses casos proceder de forma mais eficaz à pesquisa por palavras-chave.

[10] O caso Sérvulo & Associados, da Sociedade de Advogados, RL e Outros vs. Portugal, (queixa n.º 27013/10), de 3 de setembro de 2015, decorreu no âmbito de uma busca a um escritório de advogados, em que o TEDH defendeu que a pesquisa por palavras-chave que foi feita nos dispositivos encontrados nas secretárias dos advogados, foi realizada sem abusos ou violações de sigilo profissional. O JIC juntou ao processo 89 mil ficheiros apreendidos e 29 mil mensagens de correio eletrónico.

Ramos (2014) salienta que, durante uma pesquisa informática, o exame forense realizado pelos peritos, inicia-se com uma pesquisa por palavras-chave. É também captada uma imagem do suporte físico apreendido, e por fim procede-se à elaboração de um relatório pericial.

É importante salientar que o mandado judicial tem que autorizar o acesso aos servidores eletrónicos. Por sua vez, o despacho judicial prévio deve ser fundamentado, concreto e deve limitar o objeto da investigação, com base no art.º 269.º n.º 1 al. e) do CPP. A pesquisa informática tem que ser realizada de acordo com os seus requisitos, que estão presentes no art.º 15.º n.º 3 da LCC, estes são coincidentes com as formalidades apresentadas no art.º 174.º n.º 5 do CPP, para as revistas e buscas (Reis, 2023).

Neste âmbito, o Ac. do TRL, de 12/11/2019, (Cf. Proc. 71/18.3YUSTR-J.L1-PICRS), refere que o despacho judicial para a investigação do crime em causa, não continha palavras-chave que restringissem o objeto do processo e, como tal, os OPC's depararam-se com informações sobre a práticas de outros ilícitos criminais, que não se relacionavam com o crime a ser investigado. Desta forma, não foi possível aos investigadores cingir o escopo dos factos ao objeto do processo, e acabou por se aumentar a probabilidade do acesso a conhecimentos fortuitos (Reis, 2023).

Conclusão

O advento do novo milénio desencadeou transformações profundas em todas as áreas sociais, com especial foco no âmbito tecnológico, o que deu origem à sociedade da informação e da comunicação. A tecnologia permeia atualmente todas as esferas da vida social, repercutindo-se inevitavelmente no funcionamento do sistema de justiça penal. Embora o direito tenha sentido a necessidade de se adaptar, em certa medida, a esta realidade, desmaterializando documentos e integrando o digital em determinados procedimentos processuais, a verdade é que tal adaptação se tem revelado insuficiente.

A evolução tecnológica provocou inevitáveis repercussões também ao nível da criminalidade, alterando profundamente os seus métodos e formas de atuação. Perante esta realidade, a investigação criminal foi obrigada a adaptar-se, acompanhando os novos desafios mediante o recurso à ciência forense digital. Esta passou, assim, a dominar a investigação no que à prova digital diz respeito, incluindo a preservação, a recolha, a análise, a interpretação e a apreensão de elementos de prova que assumem a natureza digital.

A prova é o elemento central do processo penal e é essencial para a descoberta da verdade material e para a formação da convicção do julgador, constituindo-se como o alicerce da decisão judicial. Contudo, a obtenção da prova em ambiente digital, não pode, em circunstância alguma, subverter os direitos fundamentais consagrados constitucionalmente. Estes impõem limites materiais à atividade probatória, funcionando como garantias do Estado de direito democrático.

Os desafios inerentes à prova digital são complexos. A tutela de direitos de privacidade e as proibições de prova impõem restrições à ingerência das autoridades na esfera da vida privada dos indivíduos. Assim, está clara a intenção de o legislador proteger os dados pessoais e o conteúdo da informação contida no ambiente digital. Deve sempre existir uma ponderação de interesses, entre o direito à privacidade dos indivíduos, o interesse da investigação e do *Ius Puniendi* do Estado (Fidalgo, 2019).

A presente dissertação evidenciou que atualmente coexistem diversos regimes legais no âmbito da recolha da prova digital, designadamente no que respeita à apreensão do correio eletrónico. Os vários regimes sobrepõem-se e acabam por colidir entre si em vários aspetos, originando uma convivência normativa pouco harmoniosa e uma dificuldade acrescida na sua aplicação prática. Esta dissonância resulta, em parte, da ausência de uma regulamentação clara e sistematizada por parte do legislador, que, ora

por omissão, ora por deliberada intenção, deixou importantes zonas de incerteza jurídica por clarificar. Iremos agora, fazer uma síntese destes regimes.

A análise desenvolvida ao longo deste estudo permitiu constatar uma relevante fragmentação legal do regime jurídico da prova digital. Recuperando o argumento primordial de Correia (2014), a existência de três diplomas distintos, o CPP, a Lei n.º 32/2008 e a LCC, para regular aspetos referentes à mesma realidade, traduz-se numa assimetria jurídica e numa descentralização do CPP relativamente a uma prova que assume, cada vez mais, um papel central na investigação criminal. Esta dispersão normativa compromete a coerência legal e cria obstáculos na sua interpretação.

Com efeito, o aditamento ao CPP em 2007, veio acrescentar ao art.º 189.º a alusão de que formas de comunicação transmitidas por via telemática, onde se inclui o correio eletrónico, se devem submeter ao regime de interceção e gravação de conversações, i.e., o regime que prevê as escutas telefónicas. Desta forma, o legislador estaria a equiparar comunicações já efetuadas no ambiente digital, com uma realidade como as escutas telefónicas, que se vê extremamente mais lesiva para os direitos fundamentais, do que comunicações que já não estão em curso.

Posteriormente, foi criada a Lei n.º 109/2009, de 15 de setembro, a LCC com o intuito de dar resposta à realidade do novo século, com um regime jurídico específico para a recolha de prova em ambiente digital. No entanto, a alteração do art.º 189.º do CPP não foi expressamente anulada, nem mesmo após ter entrado em vigor um diploma legal específico para a apreensão do correio eletrónico, continuando ambas a coexistir no mesmo ordenamento jurídico, embora se encontre tacitamente revogada pelo novo normativo. A LCC prevê várias tipologias criminais no contexto da cibercriminalidade, regula o acesso e a pesquisa a dados informáticos e a sua apreensão e contempla normas relativas à cooperação internacional. O art.º 17.º desta Lei, com a epígrafe "Apreensão de correio eletrónico e registos de comunicações de natureza semelhante" permite que, mensagens, textos, ficheiros, documentos e imagens armazenadas, sejam apreendidas no âmbito da investigação (Cardoso, 2018).

Verificou-se ainda que a parte final do art.º 17.º da LCC remete para o regime da apreensão da correspondência, estabelecido no art.º 179.º n.º 1 do CPP. Ao longo do capítulo III desta dissertação foi possível analisar que a colisão destes regimes torna cada vez mais evidente a ineficiência do CPP no que toca à recolha da prova digital, pois a opção do legislador é equiparar uma mensagem de correio eletrónico à correspondência física, sem considerar a complexidade existente entre a natureza de ambas as provas.

Apesar de alguns autores defenderem que devia existir um tratamento diferente para as mensagens de correio eletrónico, diferenciando as que ainda não foram enviadas e se encontram armazenadas no operador de serviço postal, as que foram abertas e lidas e as que não foram abertas nem lidas, o art.º 17.º da LCC não faz qualquer a distinção na aplicação de regimes consoante o estado de leitura das mensagens. Conclui-se, com base na jurisprudência citada, que o visado tem o direito a não ver a sua correspondência eletrónica devassada por terceiros, independentemente de o email ter sido aberto e lido ou não. Desta forma, e privilegiando o princípio da reserva de juiz, à luz do art.º 34.º n.º 4 da CRP, deve ser o juiz de instrução o primeiro a tomar conhecimento do conteúdo das mensagens do correio eletrónico, garantindo uma proteção concisa dos direitos, liberdades e garantias dos visados.

Relativamente ao problema deste estudo, confirmamos que não existe no ordenamento jurídico português um regime de admissibilidade dos conhecimentos fortuitos relativo ao correio eletrónico, pois este conceito foi inicialmente pensado no âmbito das escutas telefónicas. Assim, a doutrina defende que se deve adaptar para a apreensão do correio eletrónico, em que se apreendem elementos que podem servir como prova em outro processo distinto, aquilo que está previsto para a admissibilidade de conhecimentos fortuitos no regime da interceção de comunicações.

Apesar da omissão legal relativamente ao uso dos conhecimentos fortuitos provenientes de uma investigação, em um processo relativo a crimes distintos, admite-se essa possibilidade, atendendo aos requisitos relevantes que foram dissecados ao longo desta dissertação, tais como, a legitimidade, o escrupuloso cumprimento do mandado de busca da investigação original, o acesso legítimo ao sistema informático, uma análise cuidada ao caso em concreto, e ao contexto em que surgiram os conhecimentos fortuitos. É importante avaliar se já existia algum grau de suspeita prévio à investigação, uma vez que não se permite uma investigação indiscriminada ao visado, devendo sempre respeitar integralmente a necessidade de um despacho judicial prévio que justifique a necessidade da investigação a partir da qual os conhecimentos fortuitos tiveram origem. A apreensão neste primeiro processo deve ser sempre validada para legitimar o uso destes conhecimentos num processo distinto. Deve existir sempre uma ponderação entre os bens jurídicos em causa, para que seja evidente que a procura pela verdade material e a realização da justiça não se podem traduzir numa violação desproporcional de direitos, liberdades e garantias.

É importante salientar que apesar da doutrina afirmar que se aplica a mesma lógica usada antes de existir uma previsão legal para a valoração de conhecimentos fortuitos nas escutas telefónicas, os requisitos não são, nem poderiam ser exatamente idênticos, pois a afetação dos bens jurídicos em causa, também não o é.

Por último, para consolidar a problemática de investigação, importa que o leitor nesta fase seja capaz de distinguir a realização de uma nova pesquisa informática ao correio eletrónico apreendido, da valoração dos conhecimentos fortuitos provenientes da apreensão feita no processo original. Sempre que existe uma nova pesquisa informática, o JIC tem que garantir que essa pesquisa tem fundamento, que respeita os direitos do arguido e que as mensagens de correio eletrónico que se vão procurar são relevantes para a descoberta da verdade ou para a prova.

A crítica substancial com que esta investigação se deparou, é que prova digital, ao invés de se encontrar integrada no corpo normativo central do processo penal, encontra-se predominantemente regulada por legislação extravagante, cuja primazia sobre o regime geral é reconhecida pela doutrina (Correia, 2014). Esta opção legislativa, embora compreensível numa perspetiva de evolução tecnológica acelerada, carece de revisão crítica, sob pena de comprometer a harmonia legal dos regimes e a eficácia da resposta jurídico-processual. Para além disto, na nossa perspetiva é urgente a criação de um regime jurídico específico e eficaz para o correio eletrónico, que atenda às especificidades da sua natureza e não o equipare a correspondência física, pois no nosso entendimento, importa sublinhar que a prova digital, pelas suas caraterísticas próprias, apresenta uma complexidade que não pode ser ignorada pelo legislador nem regulamentada à semelhança de outras provas obtidas em contexto físico.

A prova digital, pelas suas características intrínsecas, impõe desafios substanciais ao sistema de justiça penal, exigindo assim uma reconfiguração no ordenamento jurídico português.

O facto de na atualidade, se aceder remotamente, em qualquer parte do mundo a servidores informáticos, dificulta a delimitação territorial do crime e o momento exato em que foi praticado. A identificação do suspeito, por sua vez, é algo complexa, devido à possibilidade da manipulação de dados, como o endereço IP, o que dificulta a ação da investigação criminal, e torna fundamental elementos que atestem a sua autenticidade, como é o caso da verificação dos cabeçalhos técnicos do correio eletrónico.

Neste cenário, apesar da cadeia de custódia da prova digital assumir um papel determinante, por não se enquadrar no objeto central desta dissertação, não foi possível

desenvolver este tema de forma aprofundada. No entanto, pudemos perceber que é um procedimento que permite assegurar a identidade e autenticidade da prova desde o momento da sua obtenção até à sua valoração.

A jurisprudência e a doutrina convergem na necessidade de tratar a prova digital com um rigor técnico específico, exigindo-se competências informáticas por parte dos peritos na investigação criminal. Os procedimentos de recolha, apreensão, transporte, armazenamento e análise devem obedecer a determinados critérios, dado que qualquer falha na cadeia de custódia pode comprometer a descoberta da verdade material.

Neste quadro de constante evolução tecnológica, impõe-se ao legislador, bem como às autoridades judiciárias e aos OPC's a adoção de medidas estruturais e permanente formação e capacitação dos seus elementos nesta matéria, para que possam acompanhar e responder de forma eficaz aos novos desafios da era digital, garantindo que a justiça penal não só acompanhe o progresso tecnológico, como o seja capaz de fazer com rigor, coesão e segurança jurídica.

Com esta dissertação, cumpriram-se os objetivos inicialmente delineados, tendo sido possível responder ao problema de investigação proposto. Através da análise teórica e jurisprudencial, foi possível compreender a admissibilidade dos conhecimentos fortuitos no correio eletrónico. Ao longo da dissertação tornaram-se evidentes outras complexidades normativas associadas ao regime jurídico da prova digital, que, embora não constituíssem o foco central do estudo, foram essenciais para a compreensão deste tema, na medida em que permitiram o contacto com problemáticas que se mostraram fundamentais para o correto enquadramento e desenvolvimento da investigação.

Contudo, importa destacar algumas limitações da presente investigação, desde logo a escassez doutrinária e jurisprudencial relacionada com o tema, o que restringiu o campo de pesquisa e aprofundamento. Adicionalmente, o limite de extensão da dissertação impôs contenção na abordagem de certos aspetos que mereceriam maior desenvolvimento.

Como recomendações e sugestões de futuras investigações, propõe-se a análise do recurso ao *malware* como meio de obtenção de prova no processo penal, especialmente no contexto da apreensão de correio eletrónico. Outra possibilidade de evolução deste estudo passaria por uma análise de direito comparado, com o objetivo de perceber como este tema é tratado noutros ordenamentos jurídicos, o que permitiria uma visão mais alargada e enriquecedora sobre esta problemática.

Referências Bibliográficas

Aguilar, F. (2016). Notas reflexivas sobre o regime das escutas telefónicas no código de processo penal português. In J. Miranda (Ed.), *O Direito: Ano 148º* (pp. 559-584. Almedina.

Albuquerque, P. P. (2011). *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem* (4nd ed.). Universidade Católica Editora.

Almeida, I. (2018). *A prova digital*. Librum Editora.

Andrade, C. (2012). *Comentário Conimbricense do CP*. Coimbra Editora.

Andrade, M. (1992). *Sobre as proibições de prova em processo penal*. Coimbra Editora.

Andrade, M. (2009). *"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.

Brandão, D. (2019). *A prova digital no processo civil: repensar o sistema*. [Master's thesis, Universidade do Minho]. Repositório institucional da Universidade do Minho. https://repositorium.sdum.uminho.pt/bitstream/1822/74289/1/Disserta%c3%a7%c3%a3o%20Diogo%20Nuno%20Cardoso%20Miranda%20de%20Matos%20Brand%c3%a3o.pdf

Canotilho, J. J. G. & Moreira, V. (2007). *CRP anotada* (4nd ed). Coimbra Editora.

Cardoso, R. (2018). Apreensão de correio eletrónico e registos de comunicações de natureza semelhante. *Revista do Ministério Público 1*(153), 167-214.

Cardoso, R. (2019) *Apreensão de mensagens de correio eletrónico e de natureza semelhante, Direito probatório, Substantivo e Processual Penal.* Centro de Estudos Judiciários.

Casabona, C. (2006). La proteccíon penal de las mensajes de correio eletrónico y de outras comunicaciones de carácter personal a través de internet. *Derecho y conocimiento*, *(2),* 123-149.

Clemente, E. (2021). *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).* [Master's thesis, Universidade Católica Portuguesa]. Repositório Científico e Institucional da Universidade Católica Portuguesa.

Clemente, E. (2022). A *prova digital em processo penal: Apreensão de correio eletrónico.* [Master's thesis, Universidade Católica Portuguesa]. Repositório Institucional da Universidade Católica. https://repositorio.ucp.pt/bitstream/10400.14/39915/1/203156170.pdf

Contardo, R. W. (2020). Apreensão de correio eletrónico em Portugal: Presente e futuro de uma questão de "manifesta simplicidade". *Novos desafios da prova penal, 1*(1), 277-313.

Correia, J. (2014). Prova digital: As Leis que temos e a Lei que devíamos ter. *Revista do Ministério Púiblico, 139*(3), 29-59.

Correia, J. (2022). Art.º 179.º Apreensão de Correspondência. In A. Gama, A. Latas, J. Correia, J. Lopes, L. Triunfante, M. Dias, P. Mesquita, P. Albergaria, & T. Milheiro, (4nd ed.), *Comentário Judiciário do Código de Processo Penal tomo II.* Almedina.

Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24 de fevereiro. *Jornal Oficial da União Europeia.* n.º L 69/67. Conselho da União Europeia.

Dias, J. (1987). *O Novo Código de Processo Penal.* Textos Jurídicos I, Ministério da Justiça.

Dias, J. (2004). *Direito Processual Penal.* Coimbra Editora.

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

Fidalgo, S. (2022). A utilização de inteligência artificial no âmbito da prova digital: direitos fundamentais (ainda mais) em perigo. In A. Rodrigues, *A inteligência artificial no direito penal* (129-161). Almedina.

Filiol, E. (2005). *Computer viruses: from theory to applications*. Spienger.

Gonçalves, M. (2024). *Ciberdireito: Liberdades, direitos e regulação na era digital*. Almedina.

Hassemer, W. (1990). *Unferfugbares im strafprozes*. Fest Maihofer.

Hermeiro, A. (2023). *A cadeia de custódia da prova digital: o uso da tecnologia blockchain como forma de preservação*. [Master's thesis, Faculdade de Direito da Universidade de Coimbra]. Repositório Científico de cesso Aberto de Portugal. https://estudogeral.uc.pt/retrieve/259007/Dissertac%cc%a7a%cc%83o_AndreiaHermeiro.pdf

Jarrett, H., Bailie, M. (2009). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Office of Legal Education Executive Office for United States Attorneys.

Junior, W. (2021). *A utilização de malware em investigações criminais em face do estabelecido pelos direitos fundamentais.* [Master's thesis, Nova School Of Law]. Repositório Científico de Acesso Aberto de Portugal. https://run.unl.pt/bitstream/10362/142099/1/Junior_2022.pdf

Lei n.º 109/2009, de 15 de setembro. Lei do Cibercrime. *Diário da República*, n.º 179/2009, Série I de 2009-09-15. https://www.pgdlisboa.pt/Leis/Lei_mostra_articulado.php?nid=1137&tabela=Leis

Lei n.º 27/2021, de 17 de maio. Carta portuguesa de direitos humanos na era digital. *Diário da República* n.º 95/2021, Série I de 2021-05-17. https://diariodarepublica.pt/dr/detalhe/Lei/27-2021-163442504

Lei n.º 32/2008, de 17 de julho. Conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas. *Diário da República*, n.º 137/2008, Série I de 2008-07-17. https://diariodarepublica.pt/dr/detalhe/Lei/32-2008-456812

Lei n.º 5/2002, de 11 de janeiro. *Diário da República,* n.º 9/2002, Série I-A.

Lei n.º 53/2007, de 31 de agosto. *Diário da República.* Série I, n.º 168/2007.

Lei nº 109/2009, de 15 de setembro. *Diário da República*. Série I, n.º 179/2009.

Lopes, J., Cabreiro, C. (2006). A Emergência da Prova Digital na Investigação da Criminalidade Informática, *Sub Judice Justiça e Sociedade*, (35nd ed.). Almedina.

Meireles, A. I. D. (2023). *A prova digital no processo judicial: A blockchain e outros caminhos para os tribunais*. Edições Almedina, S.A.

Mendes, P. S. (2021). A privacidade digital posta à prova no processo penal. *Revista do Ministério Público, 165*(2), 225-250.

Mesquita, P. D. (2010). *Processo penal, prova e sistema judiciário.* Coimbra Editora.

Militão, R. L. (2012). A propósito da prova digital no processo penal. *Revista da Ordem dos Advogados,* 1(72), 247-285.

Monteiro, A. P. (2023). Garantias processuais e prova digital. *Revista da Ordem dos Advogados, 4*(1), 551-567.

Morim, J. (2022). *Apreensão de mensagens de correio eletrónico e a temática dos conhecimentos fortuitos.* [Master's thesis, Universidade de Coimbra]. Repositórios Científicos de Acesso Aberto de Portugal. https://estudogeral.uc.pt/retrieve/250691/Je%CC%81ssica%20B.%20Marques%20Morim%20-%20Dissertac%CC%A7a%CC%83o%20de%20Mestrado.pdf

Neves, A. B. (2012). Da utilização dos conhecimentos fortuitos obtidos através de escutas telefónicas. *Terra de Lei, 1*(2), 68-82.

Neves, R. (2011). *As ingerências nas comunicações eletrónicas em processo penal, Natureza e respectivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*. Coimbra Editora.

Núcleo de Polícia Técnica Forense. (2015). *Manual de recolha de cabeçalhos técnicos de mensagens de correio eletrónico.*

Nunes, D. (2021). *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime.* Gestlegal.

Pinheiro, A. S., Fernandes, M. (1999). *Comentário à IV Revisão Constitucional*, AAFDL Editora.

Portugal. (1976). *CRP* (8ª revisão constitucional 2005). *Diário da República*, Lei Constitucional n.º 1/2005, de 12 de agosto. https://www.pgdlisboa.pt/Leis/Lei_mostra_articulado.php?nid=4&tabela=Leis

Portugal. (1987). *Código de Processo Penal* (versão atualizada). *Diário da República*, Decreto-Lei n.º 78/87, de 17 de fevereiro. https://www.pgdlisboa.pt/Leis/Lei_mostra_articulado.php?nid=199&tabela=Leis

Ramalho, D. S. (2017). *Métodos ocultos de Investigação Criminal em Ambiente Digital.* Coimbra: Almedina.

Ramos, A. D. (2011). *Do correio tradicional ao correio eletrónico: Contributo para o estudo do fluxo informacional como meio de prova em direito penal.* [Unpublished master's thesis]. Faculdade de Direito da Universidade de Lisboa.

Ramos, A. D. (2014). *A prova digital em processo penal: O correio eletrónico.* Chiado Editorial.

Reale, M. (2010). *Filosofia do Direito*. Editora Saraiva.

Reis, J. B. (2023). O regime jurídico dos conhecimentos fortuitos em ambiente digital: contributo da plain view doctrine à luz da legislação portuguesa. *Novos desafios da prova penal, I*(1), 347-410.

Resolução da Assembleia da República n.º 88/2009, de 15 de setembro. *Diário da República.* Série I, n.º 179/2009.

Ribeiro, M. (2015). *Cibercrime e Prova Digital.* [Master's thesis, Instituto Superior Bissaya Barreto]. Repositório Científico de Acesso Aberto de Portugal. https://r.search.yahoo.com/_ylt=AwrFFm59jOVnpNoD4zJXNyoA;_ylu=Y29sbwNiZjEEcG9zAzEEdnRpZAMEc2VjA3Ny/RV=2/RE=1744306558/RO=10/RU=ht

tps%3a%2f%2fcomum.rcaap.pt%2fbitstream%2f10400.26%2f28946%2f1%2fCibercrime%2520e%2520Prova%2520Digital.pdf/RK=2/RS=PRQJOgWO1aickWuunhmKq7Joqgs-

Rodrigues, B. S. (2009). *Das escutas telefónicas tomo II: à obtenção da prova em ambiente digital* (2nd ed.). Coimbra Editora.

Ruço, A. (2017). *Prova e formação da convicção do juiz*. (2nd ed.). Almedina.

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

Silva, G. (2008). *Curso de Processo Penal.* (4nd ed.). Editorial Verbo.

Supremo Tribunal de Justiça. (2023). Ac. do Supremo Tribunal e Justiça n.º 10/2023. *Diário da República*, 1.ª série, n.º 218. (Proc. n.º 184/12.5TELSB-R.L1-A.S1). https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/10-2023-224081976

Supremo Tribunal de Justiça. (2023). Acórdão n.º 10/2023, de 11 de outubro de 2023. *Diário da República*, 1.ª série, n.º 195. (Proc. n.º 184/12.5TELSB-R.L1-A.S1). https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/10-2023-224081976Diário da República+6Diário da República+6Diário da República+6

Supremo Tribunal de Justiça. (2024). Ac.do STJ n.º 12/2024. *Diário da República*, 1.ª série, n.º 183, de 2024-09-20. (Proc. n.º 28999/18.3T8LSB-B.L1-A.S1). https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/12-2024-888344732

Supremo Tribunal de Justiça. (2024). Acórdão n.º 12/2024, de 20 de setembro de 2024. *Diário da República*, 1.ª série, n.º 183. (Proc. n.º 28999/18.3T8LSB-B.L1-A.S1).

https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/12-2024-888344732

Tribunal Constitucional. (1992). Acórdão n.º 128/92, de 24 de julho de 1992. (Proc. n.º 260/90). https://www.tribunalconstitucional.pt/tc/acordaos/19920128.htmlDiário da República+5Tribunal Constitucional+5Tribunal Constitucional+5

Tribunal Constitucional. (2021). *Acórdão n.º 687/2021, de 29 de julho de 2021*. (Proc. n.º 830/2021). https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html

Tribunal da Relação de Coimbra. (2024). *Acórdão n.º 1272/20.0T8LRA-A.C1*. https://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/b7fc034b80d07a9e80258c9900547835?OpenDocument

Tribunal da Relação de Évora. (2011). *Acórdão de 29 de março de 2011*. (Proc. N.º 77/14.1GESTC.E1). https://www.dgsi.pt/jtre.nsf/-/0373D664E6FF96998025815C004CE6BBDGSI+18DGSI+18DGSI+18

Tribunal da Relação de Évora. (2015). *Acórdão de 20 de janeiro de 2015* (Proc. n.º 648/14.6GCFAR-A.E1). https://diariodarepublica.pt/dr/detalhe/acordao/648-2015-93914375Diário da República+7Diário da República+7Diário da República+7

Tribunal da Relação de Guimarães. (2011). *Acórdão de 29 de março de 2011* (Proc. n.º 735/10.0GAPTL-A.G1). https://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument

Tribunal da Relação de Lisboa. (2007). *Acórdão de 13 de setembro de 2007*. (Proc. N.º 279/12.7YIPRT.L1-6).

https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/22b1f7b542f965ea80257bbb003d7f0c?OpenDocumentDGSI

Tribunal da Relação de Lisboa. (2009). *Acórdão de 15 de dezembro de 2009*. (Proc. n.º 629/04.8PASXL.L1-5). https://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/3a5d214e16b9df818025781b004ef022?OpenDocumentgde.mj.pt+11DGSI+11DGSI+11

Tribunal da Relação de Lisboa. (2011). *Acórdão de 11 de janeiro de 2011* (Proc. n.º 5.4.12.08.9TDLSV-A.L1-5). https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d26c12b4ce42e24a80257c69005eaa33?OpenDocumentDGSI+10DGSI+10DGSI+10

Tribunal da Relação de Lisboa. (2012). *Acórdão de 29 de março de 2012*. (Proc. n .º 14013/17.0T8LSB.L1-6). https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/3ea1614722133a00802584b60031079c?OpenDocumentDGSI

Tribunal da Relação de Lisboa. (2018). *Acórdão de 6 de fevereiro de 2018*. (Proc. n.º 195/15.9T8AMD-D.L1-2). https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/0ade0430167c8e5c802583230030f442?OpenDocumentDGSI

Tribunal da Relação de Lisboa. (2018). *Acórdão de 7 de março de 2018*. (Proc. n.º 497/15.4T9BRR.L1-9). https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/78e00ddd365f551a8025887600519fe9?OpenDocumentDGSI

Tribunal da Relação de Lisboa. (2019). *Acórdão de 11 de julho de 2019*. (Proc. nº 184/12.5TELSB-B.L1-3). https://diariodarepublica.pt/dr/detalhe/acordao/184-2019-190275975Diário da República+7Diário da República+7Diário da República+7

Tribunal da Relação de Lisboa. (2019). *Acórdão de 12 de novembro de 2019*. (Proc. n.º 4013/15.0T8LRS.L1-7). https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1efdd096db6363db8025843b0031e0fb?OpenDocumentDGSI+21DGSI+21DGSI+21

Tribunal da Relação do Porto. (2013). *Acórdão de 22 de maio de 2013*. (Proc. n.º 1/22.8GAPNF.P1). https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/5755c968300ff52080258b5f00560250?OpenDocumentDGSI

Valente, M. (2004). *Escutas Telefónicas – Da Excepcionalidade à Vulgaridade* (2nd ed.)., Almedina.

Valente, M. (2019). *Cadeia de custódia da prova*, Coimbra: Almedina.

Valente, M. (2021). *Cadeia de Custódia da Prova* (3nd ed). Edições Almedina.

Valente, M. M. G. (2019). *Teoria Geral do Direito Policial* (6ª Ed.). Almedina.

Venâncio, P. D. (2023). *LCC: Anotada e comentada - Atualizada pela Lei n.º 79/2021, de 24 de novembro*. Editora D'Ideias.

Verdelho, P. (2004). Apreensão de Correio Eletrónico em Processo Penal, in *Revista do Ministério Público n .º100.*

Verdelho, P. (2009). A Nova LCC. *Revista de Direito Comparado Português e Brasileiro*. Scientia Ivridica. Universidade do Minho.

Verdelho, P., Bravo, R., Rocha, M., (2003). *Leis do Cibercrime*. Edições Centro Atlântico.