

Universidades Lusíada

Santos, Samanta Alexandra de Sousa, 2000-

Procedimento da apreensão do correio eletrónico e registos de comunicação de natureza semelhante, à luz do artigo 17.º da lei do cibercrime

<http://hdl.handle.net/11067/8677>

Metadados

Data de Publicação

2025

Resumo

A presente dissertação tem como objetivo a análise do procedimento de apreensão do correio eletrónico e dos registos de comunicação de natureza semelhante, à luz do artigo 17º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), enquadrando-o no contexto do Direito Processual Penal. O estudo inicia-se com a definição de prova digital, analisando-se a sua natureza jurídica e a relevância do correio eletrónico como meio de comunicação com valor probatório, com a devida distinção entre as m...

The aim of this dissertation is to analyse the procedure for seizing electronic mail and communication records of similar nature, in the light of Article 17 of the Cybercrime Law (Law no. 109/2009, of 15 September), placing it in the context of criminal procedural law. The study begins with the definition of digital evidence, analysing its legal nature and the relevance of electronic mail as a means of communication with probative value with a proper distinction between messages sent, received,...

Palavras Chave

Prova digital - Portugal, Direito à privacidade, Prova digital – Espanha, Prova digital – Alemanha, Mensagens de correio eletrónico - Direito e legislação, Crimes informáticos - Direito e legislação

Tipo

masterThesis

Revisão de Pares

Não

Coleções

[ULL-FD] Dissertações

Esta página foi gerada automaticamente em 2026-10-30T03:39:57Z com informação proveniente do Repositório



UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

**Procedimento da apreensão do correio eletrónico e
registos de comunicação de natureza semelhante,
à luz do artigo 17.º da lei do cibercrime**

Realizado por:

Samanta Alexandra de Sousa Santos

Orientado por:

Professora Doutora Ana Bárbara Pina de Morais de Sousa e Brito

Constituição do Júri:

Presidente:	Professor Doutor José Alberto Rodríguez Lorenzo González
Orientadora:	Professora Doutora Ana Bárbara Pina de Morais de Sousa e Brito
Arguente:	Professora Doutora Maria Leonor Machado Esteves

Dissertação aprovada em: 10 de março de 2026

Lisboa

2025



U N I V E R S I D A D E L U S Í A D A

FACULDADE DE DIREITO

Mestrado em Direito

Procedimento da apreensão do correio eletrónico e
registos de comunicação de natureza semelhante,
à luz do artigo 17.º da lei do cibercrime

Samanta Alexandra de Sousa Santos

Lisboa

Agosto 2025



U N I V E R S I D A D E L U S Í A D A

FACULDADE DE DIREITO

Mestrado em Direito

Procedimento da apreensão do correio eletrónico e
registos de comunicação de natureza semelhante,
à luz do artigo 17.º da lei do cibercrime

Samanta Alexandra de Sousa Santos

Lisboa

Agosto 2025

Samanta Alexandra de Sousa Santos

Procedimento da apreensão do correio eletrónico e
registos de comunicação de natureza semelhante,
à luz do artigo 17.º da lei do cibercrime

Dissertação apresentada à Faculdade de Direito da
Universidade Lusíada para a obtenção do grau de
Mestre em Direito.

Área científica: Ciências Jurídico-Criminais

Orientadora: Professora Doutora Ana Bárbara Pina de
Morais de Sousa e Brito

Lisboa

Agosto 2025

FICHA TÉCNICA

Autora Samanta Alexandra de Sousa Santos
Orientadora Professora Doutora Ana Bárbara Pina de Morais de Sousa e Brito
Título Procedimento da apreensão do correio eletrónico e registos de comunicação de natureza semelhante, à luz do artigo 17.º da lei do cibercrime
Local Lisboa
Ano 2025

CASA DO CONHECIMENTO DA UNIVERSIDADE LUSÍADA - CATALOGAÇÃO NA PUBLICAÇÃO

SANTOS, Samanta Alexandra de Sousa, 2000-

Procedimento da apreensão do correio eletrónico e registos de comunicação de natureza semelhante, à luz do artigo 17.º da lei do cibercrime / Samanta Alexandra de Sousa Santos ; orientado por Ana Bárbara Pina de Morais de Sousa e Brito. - Lisboa : [s.n.], 2025. - Dissertação de Mestrado em Direito, Faculdade de Direito da Universidade Lusíada.

I - BRITO, Ana Bárbara Pina de Morais de Sousa e, 1970-

LCSH

1. Prova digital - Portugal
2. Prova digital - Espanha
3. Prova digital - Alemanha
4. Mensagens de correio eletrónico - Direito e legislação
5. Direito à privacidade
6. Crimes informáticos - Direito e legislação
7. Universidade Lusíada. Faculdade de Direito - Teses
8. Teses - Portugal - Lisboa

1. Electronic evidence - Portugal
2. Electronic evidence - Spain
3. Electronic evidence - Germany
4. Electronic mail messages - Law and legislation
5. Privacy, Right of
6. Computer crimes - Law and legislation
7. Universidade Lusíada. Faculdade de Direito - Dissertations
8. Dissertations, academic - Portugal - Lisbon

LCC

1. KKQ4679.S26 2025

AVISO LEGAL

O conteúdo desta dissertação reflete as perspetivas, o trabalho e as interpretações da autora no momento da sua entrega. Esta dissertação pode conter incorreções, tanto conceptuais como metodológicas, que podem ter sido identificadas em momento posterior ao da sua entrega. Por conseguinte, qualquer utilização dos seus conteúdos deve ser exercida com cautela. Ao entregar esta dissertação, a autora declara que a mesma é resultante do seu próprio trabalho, contém contributos originais e são reconhecidas todas as fontes utilizadas, encontrando-se tais fontes devidamente citadas no corpo do texto e identificadas na secção de referências. A autora declara, ainda, que não divulga na presente dissertação quaisquer conteúdos cuja reprodução esteja vedada por direitos de autor ou de propriedade industrial.

Agradecimentos

À minha família que me apoiou em todos os meus passos, tanto a nível pessoal como a nível académico, quero agradecer pelas palavras de apoio e pelo carinho e amor incondicional.

Aos amigos que me apoiaram nesta jornada difícil e até mesmo aqueles que estavam na mesma situação que a minha, principalmente, à minha amiga M. por me ter aturado em vários momentos.

Para finalizar estes agradecimentos, quero agradecer à minha orientadora Professora Doutora Ana Bárbara de Sousa e Brito pela sua disponibilidade em ajudar me nesta fase e pelos conselhos e instruções que me deu.

Apresentação

Procedimento da apreensão do correio eletrónico e registos de comunicação de natureza semelhante, à luz do artigo 17.º da Lei do Cibercrime

Samanta Alexandra de Sousa Santos

A presente dissertação tem como objetivo a análise do procedimento de apreensão do correio eletrónico e dos registos de comunicação de natureza semelhante, à luz do artigo 17º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), enquadrando-o no contexto do Direito Processual Penal.

O estudo inicia-se com a definição de prova digital, analisando-se a sua natureza jurídica e a relevância do correio eletrónico como meio de comunicação com valor probatório, com a devida distinção entre as mensagens enviadas, as recebidas, as lidas e não lidas, assim como outras formas de registos de comunicação de natureza semelhante realizadas através da internet.

A investigação inclui uma análise da evolução legislativa nacional e internacional que esteve na origem da Lei do Cibercrime, destacando-se com especial atenção à Convenção de Budapeste, à Decisão-Quadro 2005/222/JAI e à Diretiva (UE) 2016/680. O estudo integra ainda um enquadramento constitucional, abordando os direitos fundamentais em causa, nomeadamente, o direito à privacidade, à inviolabilidade das comunicações e à proteção de dados pessoais dos cidadãos.

Dar-se-á destaque à forma que os tribunais têm resolvido a distinção entre o correio aberto e fechado, pois existe uma diversidade de opiniões quanto à proteção jurídica aplicável.

Por fim, procede-se a uma comparação com os ordenamentos jurídicos da Alemanha e de Espanha, identificando os procedimentos e as soluções legislativas para a recolha de prova digital, mais precisamente, a apreensão do correio eletrónico e de registos de comunicação de natureza semelhante, relacionando-as com o regime vigente no ordenamento jurídico português.

Palavras-chave: Prova Digital, Direito Processual Penal, Privacidade, Correio Eletrónico, Registos de Comunicação, Cibercrime.

Presentation

Procedure for the seizure of electronic mail and communication records of a similar nature, in the light of article 17 of the Cybercrime Law

Samanta Alexandra de Sousa Santos

The aim of this dissertation is to analyse the procedure for seizing electronic mail and communication records of similar nature, in the light of Article 17 of the Cybercrime Law (Law no. 109/2009, of 15 September), placing it in the context of criminal procedural law. The study begins with the definition of digital evidence, analysing its legal nature and the relevance of electronic mail as a means of communication with probative value with a proper distinction between messages sent, received, read and unread, as well as other forms of communication records of a similar nature made over the internet.

The research includes an analysis of the national and international legislative developments that gave rise to the Cybercrime Law, with particular attention to the Budapest Convention, Framework Decision 2005/222/JHA and Directive (EU) 2016/680. The study also includes a constitutional framework, addressing the fundamental rights in question, namely the right to privacy, the inviolability of communications and the protection of citizens personal data.

Emphasis will be placed on how the courts have resolved the distinction between open and closed mail, as there is a diversity of opinions regarding the applicable legal protection.

Finally, a comparison is made with the legal systems of Germany and Spain, identifying the procedures and legislative solutions for the collection of digital evidence, more precisely, the seizure of electronic mail and communication records of a similar nature, relating them to the system in force in the Portuguese legal system.

Keywords: Digital Evidence, Criminal Procedure Law, Privacy, Electronic Mail, Communication Records, Cybercrime.

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

Al. – Alínea

Apud – Junto de/ em

Art./Arts. - Artigo / Artigos

Cit. – Citação

CP - Código Penal

CPP - Código de Processo Penal

CRP - Constituição da República Portuguesa

Ed. – Edição

Ibidem – No mesmo Lugar

Idem – O mesmo

JIC – Juiz de Instrução Criminal

MP – Ministério Público

N.º/N.ºs - Número / Números

P. – Página

PP. – Páginas

Ob. – Obra

SS. – Seguintes

STJ - Supremo Tribunal de Justiça

StPO - Strafprozeßordnung – Código de Processo Penal Alemão

TC - Tribunal Constitucional

TRE - Tribunal da Relação de Évora

TRG - Tribunal da Relação de Guimarães

TRL - Tribunal da Relação de Lisboa

TEDH - Tribunal Europeu dos Direitos Humanos

TFUE - Tratado sobre o Funcionamento da União Europeia

Sumário

Introdução.....	12
Capítulo 1: Conceitos relevantes no âmbito da apreensão do correio eletrónico e registo de comunicações relevantes	14
1. Prova digital	14
2. Correio eletrónico.....	16
2.1 Mensagens enviadas e recebidas	17
2.2 Mensagens abertas e mensagens fechadas	20
3. Comunicações de natureza semelhante.....	22
Capítulo 2: Evolução do tratamento legislativo da apreensão de correio eletrónico e registos de comunicação de natureza semelhante	25
1. Código Processo Penal antes de 2009.....	25
2. Diplomas internacionais na base da Lei do Cibercrime (Lei n.º 109/2009 de 15 de setembro).....	26
2.1 Convenção de Budapeste sobre o cibercrime	27
2.2 Decisão-Quadro 2005/222/JAI do Conselho da União Europeia	30
2.3 Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016	31
Capítulo 3: Análise do artigo 17º da Lei do Cibercrime	33
1. Generalidades.....	33
2. Lista de crimes que permitem a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante	37
3. Remissão para o artigo 179º do CPP	39
3.1 Competência para autorizar a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante.....	44
3.2 Situações de <i>periculum in mora</i>	50
3.2.1 Posterior valoração das provas obtidas neste modo	54
4. Grau de suspeita exigido para o procedimento do respetivo artigo.....	55
Capítulo 4: Enquadramento jurídico-constitucional deste meio de prova	58

1. Direito fundamental à reserva da vida privada	58
2. Proteção da palavra escrita e da palavra falada.....	59
3. Princípio da proporcionalidade	61
4. Proteção de dados pessoais (CDFUE) e Privacidade (CEDH)	62
Capítulo 5: Tratamento jurisprudencial deste meio de obtenção de prova	67
1. Divergência no tratamento a dar ao correio aberto e fechado.....	67
1.1 Tomada de posição	76
Capítulo 6: O procedimento noutros ordenamentos jurídicos	79
1. Alemanha.....	79
2. Espanha.....	83
Conclusão.....	88
Bibliografia	93

Introdução

A presente dissertação tem como principal objetivo analisar, de forma detalhada, o procedimento da apreensão do correio eletrónico e dos registos de comunicação de natureza semelhante, cujo regime se encontra previsto no artigo 17.º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro).

O estudo parte da necessidade de compreender de que forma este meio de obtenção de prova se enquadra no âmbito do Direito Processual Penal, devido à sua característica particular e à relevância prática que tem assumido, sobretudo face à constante evolução tecnológica e aos desafios que são causados pela mesma.

Num primeiro momento, procede-se à clarificação dos conceitos fundamentais que acabam por sustentar esta análise, nomeadamente, o de prova digital e o de correio eletrónico, destacando-se as diferentes espécies de mensagens, desde logo, as enviadas, as recebidas abertas ou não lidas, assim como outras formas de comunicação análogas.

Em seguida, será abordada a evolução legislativa, tanto a nível nacional como internacional, com especial atenção à Convenção de Budapeste, que trata da criminalidade informática, à Decisão-Quadro 2005/222/JAI do Conselho da União Europeia, que harmoniza a legislação penal europeia e à Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016, que regula o tratamento de dados pessoais no âmbito penal, ou seja, são normas que influenciam decisivamente a regulamentação portuguesa nesta matéria.

Esta dissertação irá dar especial atenção à análise do artigo 17.º da Lei do Cibercrime, abordando os critérios legais de admissibilidade desta prova, a remissão para o artigo 179.º do Código de Processo Penal, especificar as competências atribuídas às autoridades judiciais e as questões suscitadas em situações de urgência, sem deixar de referenciar o princípio da descoberta da verdade material.

Para além da perspetiva processual, esta investigação procura também refletir sobre o enquadramento constitucional deste meio de prova, com destaque para os direitos fundamentais que podem ser postos em causa com este meio de prova, como a reserva da vida privada, a proteção da palavra escrita e da palavra falada, para o princípio da proporcionalidade, e por fim, para a proteção de dados pessoais.

No quinto capítulo deste trabalho, será realizada uma análise da nossa jurisprudência nomeadamente sobre a distinção entre o correio aberto e fechado, mostrando a existência de diferentes interpretações doutrinárias sobre o tema e alcançar uma interpretação mais coerente com as normas.

Por fim, será realizada uma análise dos ordenamentos jurídicos da Alemanha e de Espanha, referindo as suas soluções normativas e práticas uma vez que estes ordenamentos servem como reflexão para o sistema jurídico português.

Com este trabalho, pretende-se contribuir para uma maior clareza na aplicação das normas relacionadas com a apreensão do correio eletrónico e de registos de comunicação de natureza semelhante e, conseqüentemente, perceber de forma aprofundada como devem as autoridades competentes proceder até ao momento da referida apreensão.

Pretende-se, assim, esclarecer não só os critérios legais e práticos que orientam a atuação do Ministério Público, dos órgãos de polícia criminal e do juiz de instrução criminal, mas também refletir sobre os limites impostos pelos direitos, liberdades e garantias constitucionalmente protegidos.

Desta forma, iremos perceber que o que se procura é garantir o equilíbrio entre a eficácia da investigação criminal com a salvaguarda dos direitos fundamentais dos cidadãos e o restabelecimento da ordem jurídica da comunidade.

Este meio de obtenção de prova é cada vez mais relevante porque com a evolução da tecnologia e da comunicação o cibercrime tornou-se um fenómeno complexo e desafiante para os ordenamentos jurídicos, sobretudo quando estão em causa crimes de elevada gravidade e complexidade devido à facilidade com que se enviam e armazenam mensagens de correio eletrónico e pela diversidade de aplicações de mensagens instantâneas.

Tudo isto, ainda levanta o problema da encriptação de ponta-a-ponta, que dificulta a recolha de prova digital durante a investigação criminal e, conseqüentemente, faz com que os Estados, em especial, os da União Europeia, tenham de adaptar os seus regulamentos e procedimentos de investigação, sempre sem violarem os direitos fundamentais dos cidadãos.

Capítulo 1: Conceitos relevantes no âmbito da apreensão do correio eletrónico e registo de comunicações relevantes

1. Prova digital

O Direito Digital é um ramo do direito que, conseqüentemente, surgiu através da relação entre a ciência do Direito e da ciência da Computação, ou seja, através do “conjunto de relações jurídicas, normas aplicações e conhecimentos que sejam oriundas do mundo digital e cuja regulação se impõem, hoje mais que nunca.”¹.

Este ramo surgiu devido à necessidade de acompanhar os avanços tecnológicos e pelas transformações causadas pela nossa era digital.

No entanto, tem como objetivo dar resposta a novos desafios que vão aparecendo com a evolução da internet, das redes sociais, e das formas diversas como hoje nos comunicamos e como trabalhamos.

São vários os temas que podem ser alvo de questões, desde a proteção de dados pessoais, aos crimes informáticos e à cibersegurança, pois são pontos que estão sempre em processo de evolução e que podem ser facilmente violados no mundo do crime.

Esta área do Direito está necessariamente relacionada com matérias de outros ramos do ordenamento jurídico, desde logo, o Direito Penal (ex.: Lei do Cibercrime), o Direito Civil, o Direito do Trabalho, Direito Fiscal, o Direito Comercial e, por fim, o Direito Constitucional².

Ora, o Direito Digital está sempre em processo de evolução, exigindo uma atualização contínua da legislação e da jurisprudência, mas também uma abordagem interdisciplinar, ou seja, não basta o conhecimento jurídico do direito para lidar com os desafios colocados pelas novas tecnologias é também necessário a colaboração de diferentes áreas do saber, neste caso, compreensão técnica das tecnologias digitais (ex.: engenharia informática).

A prova digital é definida como “a informação relevante para fins probatórios produzida/obtida a partir de dados em formato digital (na forma binária, em que todas

¹ Schwalbach, José Gaspar (2021) – Direito Digital, 2ª ed., Almedina Editora, p. 35.

² Idem, *ibidem*.

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 comunicação eletrónica.”³.

Porém, a prova digital não é apenas utilizada como elemento de prova dos crimes informáticos, mas também pode ser utilizada como prova de outros crimes, tais como, o homicídio (arts. 131.º, 132.º, 133.º do CP), terrorismo, criminalidade organizada, branqueamento de capitais, armas, tráfico de estupefacientes, entre outros⁴.

Relativamente às características da prova digital, segundo o autor Duarte Nunes, esta caracteriza-se por ser imaterial e invisível, ao contrário da prova física, e por se encontrar armazenada em locais acessíveis apenas com a utilização de ferramentas próprias e apenas as pessoas que são dotadas de conhecimento sobre informática, poderão pesquisar e apreender os dados que são importantes para a descoberta da verdade⁵.

A outra característica consiste em ser volátil e frágil, pois pode ser eliminada ou manipulada quer por ação humana ou pelo próprio sistema informático (ex.: avaria, mau funcionamento, entre outras situações).

Por isso, dado à natureza da prova digital, torna-se crucial que a recolha seja feita com celeridade e correção técnica na sua obtenção, de modo a evitar a sua eliminação, alteração ou ocultação, bem como proceder à criação de uma cópia integral do sistema informático, permitindo assim uma análise forense posterior, além disso, a sua conservação deve ocorrer de forma imediata e segura, sendo frequente em alguns casos, recorrer-se à recolha remota e “às ocultas”, sem o conhecimento dos titulares ou de terceiros para não interferirem no processo de investigação⁶.

A prova digital devido à sua natureza invisível e volátil torna assim essencial que a sua recolha seja rápida e segura para evitar que os dados sejam apagados ou alterados.

Assim, tanto o Direito Digital como prova digital demonstram a importância de adaptar o sistema jurídico às novas realidades da tecnologia, garantindo a proteção dos direitos, mas também a eficácia da justiça na descoberta da verdade.

³ Nunes, Duarte Rodrigues (2021) - Os meios de obtenção de prova previstos na Lei do Cibercrime, 2ª ed. Gestlegal Editora, p. 47.

⁴ No mesmo sentido de Nunes, Duarte Rodrigues, (2021), p. 47.

⁵ Idem, pp. 48 e 49.

⁶ Idem, *ibidem*.

2. Correio eletrónico

Antes de abordarmos o regime específico da apreensão do correio eletrónico e de registos de comunicação de natureza semelhante, vamos começar por analisar o conceito de correio eletrónico como meio de prova.

Nos finais dos anos 60, com a criação dos computadores, a comunicação à distância tornou cada vez mais rápida e também segura⁷.

Com a evolução da Internet, enquanto meio de comunicação na sociedade atual, foi criado o serviço de correio eletrónico, sendo que anteriormente existiam, entre outros, os pombos-correio, onde a mensagem era colocada numa das suas patas e os mensageiros⁸.

Ora, o correio eletrónico ou também conhecido por e-mail (do inglês “electronic mail”), trata-se de um serviço de comunicação que permite a qualquer pessoa enviar e receber mensagens escritas e/ou anexar ficheiros, tais como, vídeos, fotografias, documentos e links, através da Internet, de uma forma mais rápida e independentemente da localização do seu destinatário, apenas será necessário possuir uma ligação à Internet e estar registado num servidor de e-mail como por exemplo, o Gmail ou o Hotmail.

Quando nos referimos que o correio eletrónico se trata de uma forma mais rápida de comunicação entre duas ou mais pessoas, deve-se ao facto de este demorar segundos a ser enviado ao seu destinatário, enquanto o correio postal, mais precisamente, por carta, pode levar dias a ser recebido.

O correio eletrónico tornou-se um dos meios de comunicação criados pelas novas tecnologias da informação e comunicação e segundo a al. b) do n.º 1 do artigo 2.º da Lei n.º 41/2004, de 18 de agosto, na redação que lhe foi dada pela Lei n.º 46/2012, de 29 de agosto, refere-o como “qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha.”

⁷ Freitas, José Pedro (2020) - Os meios de obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos serviços de Correio Eletrónico e de Mensagens Curtas, Nova Causa Editora, p. 95.

⁸ Idem, p. 95.

Já no que concerne à necessidade de uma apreensão de correio eletrónico e de registos de comunicação de natureza semelhante durante um processo de investigação criminal temos o artigo 17.º da Lei do Cibercrime.

O conceito de correio eletrónico já na visão da nossa doutrina apresenta algumas definições que variam de autor para autor.

O autor Carlos Casabona define esta comunicação como uma “modalidade de comunicação pessoal composta por ficheiros de texto, voz ou imagem usufruindo das redes telemáticas com a tecnologia de transmissão e receção dos sistemas informáticos.”⁹.

Para o autor Armando Dias Ramos, o correio eletrónico trata-se de,

Um programa informático que permite a comunicação instantânea, de modo diferenciado, entre quem a envia e quem a recebe, através das redes de informação e comunicação, independentemente do local onde se encontrem, sem a necessidade deste se encontrar instalado no computador.¹⁰.

Exposto isto, entendemos que o serviço de correio eletrónico se trata de um meio de comunicação rápido, entre duas ou mais pessoas, em que a mensagem não terá de ser apenas na forma de texto, mas também, na forma de voz, som e imagem.

Este meio de comunicação pode ser apreendido pelas entidades competentes durante um processo de investigação criminal, tendo em conta desde logo o artigo 17.º da Lei do Cibercrime que faz remissão para o artigo 179.º do CPP.

2.1 Mensagens enviadas e recebidas

O correio eletrónico pode ser utilizado durante 24 horas por dia, ao contrário do correio postal que depende de ação direta de pessoas e com horas específicas para a entrega/envio¹¹.

⁹ Idem, pp. 96 e 97 *apud* Casabona, Carlos María Romeo (2002) - “la protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet”, Derecho y Conocimiento, Vol. 2, p. 129.

¹⁰ Idem, pp. 97 *apud* Ramos, Armando Dias Ramos (2014) - A Prova Digital em Processo Penal: O correio eletrónico, 2ª ed. Chiado Editora, p. 25.

¹¹ Idem, p. 96.

Quando o remetente acaba de escrever ou anexar um ficheiro, este irá enviar/encaminhar o correio eletrónico para o respetivo destinatário e depois é recebido e lido por este último, no entanto, quando transmitidas pela Internet, a mensagem de correio eletrónico contém conteúdo (e.g. texto e ficheiros em anexo), e dados de tráfego¹² que segundo a al. c) do artigo 2.º da Lei n.º 109/2009, de 15 de setembro, consiste em “dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.”

O mesmo acontece quando enviamos um SMS, ou até mesmo uma mensagem, por exemplo, no WhatsApp.

Importa também referir, que estas mensagens podem ser encriptadas de ponta-a-ponta, isto é, utilizar-se um método de segurança em que apenas o remetente e o destinatário podem ler as mensagens que partilharam, sem que nenhum terceiro as possa aceder, existindo assim um reforço na privacidade e na segurança da comunicação digital.

A criptografia de ponta a ponta (E2EE) consiste em um processo de comunicação seguro que criptografa dados antes de serem enviados para outro *endpoint*¹³, ou seja, fornece segurança de dados do início ao fim¹⁴.

Esta tem como principais benefícios a segurança de dados, a privacidade de dados, a proteção contra a vigilância de terceiros e uma resistência à adulteração tornando-a, assim, fundamental para assegurar as comunicações digitais, proteger informações confidenciais e garantir a integridade da transmissão de dados¹⁵.

Os órgãos policiais demonstram uma preocupação em relação às mensagens encriptadas, pois estas travam diversas investigações, porque as autoridades ficam sem meios para prevenir crimes mais graves, tais como, “o abuso sexual de crianças, o

¹² Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX, p. 67, [Consult. 29 out. 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>. ISBN 978-989-8908-17-9.

¹³ Trata-se de um dispositivo final que pode enviar, receber ou processar dados, que também pode ser alvo de ataques cibernéticos.

¹⁴ IBM – O que é criptografia de ponta a ponta (E2EE)? Disponível para consulta em <https://www.ibm.com/br-pt/topics/end-to-end-encryption>.

¹⁵ IBM – O que é criptografia de ponta a ponta (E2EE)? Disponível para consulta em <https://www.ibm.com/br-pt/topics/end-to-end-encryption>.

tráfico de seres humanos, contrabando de droga, o homicídio, a criminalidade económica e o terrorismo.”¹⁶.

Tendo em conta esta situação, resta às autoridades utilizarem outras estratégias, tais como, a análise de metadados (Lei n.º 18/2024, de 05 de fevereiro) que inclui informações do remetente e do destinatário, registos de data e hora, permitindo por vezes, revelar padrões e conexões entre pessoas, embora o conteúdo das mensagens permaneça criptografado.

Tudo isto, gera um debate sobre o equilíbrio entre a privacidade e a segurança, que não tem tido consenso pela sua dificuldade.

Por um lado, não se quer violar os direitos dos cidadãos e por outro não se quer dificultar o trabalho das autoridades durante as investigações, por isso, o relatório “First Report on Encryption”, publicado pelo EU Innovation Hub, realça a dificuldade em equilibrar a privacidade e a segurança em contexto da investigação criminal¹⁷.

A encriptação de ponta-a-ponta, apesar de ser essencial para garantir a confidencialidade das comunicações e a proteção dos dados pessoais, tem causado dificuldades no que toca ao acesso, pelas autoridades competentes, a provas relevantes para a descoberta da verdade, ou seja, tornam-se inacessíveis mesmo com autorização judicial.

Tal como refere o relatório, o grande desafio está em encontrar um equilíbrio que não prejudique nem enfraqueça a encriptação, mas ao mesmo tempo não impeça a investigação.

Assim um dos caminhos é o reforço da cooperação entre os legisladores, operadores tecnológicos e autoridades, promovendo soluções que respeitem tanto os direitos fundamentais dos cidadãos e a efetividade das investigações no âmbito de um processo penal.

¹⁶ Diário de notícias, disponível em <https://www.dn.pt/sociedade/europol-declara-guerra-as-mensagens-criptadas-que-travam-investigacoes-pi-juntou-se-ao-alerta>.

¹⁷ EU Innovation Hub (2024) – First Report on Encryption. Disponível em [https://www.europol.europa.eu/cms/sites/default/files/documents/EU Innovation Hub First Report on Encryption.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/EU%20Innovation%20Hub%20First%20Report%20on%20Encryption.pdf).

Porém, é ainda referido que se deve optar por uma resposta cuidadosa, proporcional e fundamentada para se evitar a violação dos direitos fundamentais consagrados na Constituição, incluindo a segurança.

Exposto isto, o correio eletrónico e as mensagens instantâneas trouxeram a facilidade e a rapidez na comunicação, mas também levantaram alguns desafios na área da segurança e na investigação criminal, desde logo, a encriptação de ponta-a-ponta que garante uma maior privacidade e proteção dos dados, o que é muito importante para uma sociedade cada vez mais digital, porém, esta mesma proteção traz dificuldades às investigações realizadas pelas autoridades, que veem os seus meios limitados mesmo em casos mais graves.

Para fazer face a esta situação é necessário existir um equilíbrio entre a privacidade dos cidadãos e a segurança, mesmo com o recurso aos metadados, que apesar de não revelarem o conteúdo das mensagens não deixam de ser úteis para a descoberta da verdade, mas esta abordagem gera algum debate.

2.2 Mensagens abertas e mensagens fechadas

Antes de avançarmos para o conceito das comunicações de natureza semelhante, vamos estudar a diferença entre as mensagens abertas ou já lidas e fechadas ou não lidas pelo seu destinatário.

Quando a mensagem se encontra fechada, o destinatário não sabe do conteúdo da mesma, nesta situação a mensagem tem na mesma proteção constitucional.

O mesmo acontece com a mensagem já aberta e lida, a única diferença é que o destinatário já sabe o conteúdo da comunicação e esta está armazenada no sistema informático, com a sua devida proteção constitucional.

Uma vez que o destinatário recebe a mensagem do remetente, essa mensagem fica depositada no servidor do primeiro e não apenas quando é descarregada para o seu computador¹⁸, telemóvel ou tablet.

¹⁸ Venâncio, Pedro Dias (2023) - Lei do Cibercrime, Anotada e Comentada, Atualizada pela Lei n.º 79/2021, de 24 de novembro, Coimbra d' Ideias Editora, p. 183.

No momento, em que a mensagem fica na posse do destinatário, este vai decidir se a vai ler ou não e ainda, depois de ler pode aceder à mesma a todo o tempo¹⁹.

Entendemos assim, que no momento, em que a mensagens fica armazenada no servidor do destinatário, esta fica ao abrigo do regime do artigo 17.º da Lei n.º 109/2009, de 15 de setembro (Apreensão de correio eletrónico e de registo de comunicação de natureza semelhante).

Apesar desta nossa posição importa referir que uma das questões controversa que se coloca sobre este tema, consiste em perceber se há necessidade ou não de haver uma distinção entre mensagens abertas ou fechadas (emails, SMS, mensagens instantâneas, etc.), para que se possa proceder à apreensão do correio eletrónico e registos de comunicação de natureza semelhante.

A outra questão que se coloca sobre este tema, das mensagens abertas e mensagens fechadas e o seu regime deve-se ao facto de o correio eletrónico não ter a mesma equiparação da correspondência tradicional, neste caso, da carta, mas, ainda assim, o artigo 17.º da Lei do Cibercrime remeter para o artigo 179.º do CPP.

Ora, para alguns autores tal não faz qualquer sentido, porque não é por o correio eletrónico “ser uma forma de correspondência, que se deva reconduzir automaticamente ao regime estabelecido para a correspondência dita tradicional”²⁰, até porque nem utiliza as redes postais públicas, como é o caso das cartas, mas sim os serviços privados de comunicações.

Além disso, se acrescenta que o artigo 179.º faz referência, principalmente, para a “apreensão de realidades físicas e não virtuais”²¹.

Iremos abordar estas duas questões mais à frente neste trabalho, com o auxílio da jurisprudência e da nossa doutrina para chegarmos a uma conclusão bem fundamentada.

¹⁹ Idem, p. 183.

²⁰ Neves, Inês Castanheira (2011) - As Ingerências nas Comunicações Electrónicas em Processo Penal, 1ª ed., Coimbra Editora, p.185.

²¹ Nunes, Duarte Rodrigues, (2021), p. 344.

3. Comunicações de natureza semelhante

Depois de termos analisado o conceito de correio eletrónico, falta entender, no que consiste as comunicações de natureza semelhante e as suas diferenças para finalizarmos este capítulo.

Atualmente, devido à evolução da tecnologia, já não é utilizado apenas o correio eletrónico como meio de comunicação entre duas ou mais pessoas, existe outras diversas formas de comunicação através de um dispositivo eletrónico com ou sem Internet.

Começaremos pela tecnologia mais antiga de mensagens de texto, que consiste num meio de comunicação, como o correio eletrónico, mas que é considerado como comunicações de natureza semelhante, e neste grupo temos, os SMS (short message service), as EMS (enhanced messaging service) e as MMS (multimedia messaging service) e para que estas sejam intercetadas devem estar ao abrigo dos artigos 187.º e 188.º do CPP²².

Os SMS e as MMS, permitem enviar mensagens de texto, arquivos de vídeo, contatos telefónicos e enviar áudios, ambos são enviados para uma rede móvel, por isso, é necessário existir um plano sem fio das operadoras de telemóvel (serviço pago), ao contrário do correio eletrónico, não é necessário fazer um download²³.

As comunicações de natureza semelhante podem também ser realizadas através de um serviço de comunicações de voz²⁴, em que uma pessoa terá de ter o seu contato telefónico ou até mesmo através da internet, caso tenha aderido ao serviço de comunicações eletrónicas, segundo o artigo 3.º, n.º 1, al. ss) da Lei das Comunicações Eletrónicas ou ainda, ter conectado o seu dispositivo eletrónico (smartphone, tablet ou computador) a uma outra rede WiFi fora de casa.

²² Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15. IX, p. 68 [Consult. 29 out, 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QG6e-U=&portalid=30>. ISBN 978-989-8908-17-9.

²³ TWILIO – Mensagens. Disponível em <https://www.twilio.com/pt-br/learn/messaging/what-are-sms-and-mms> [Consult. 30 out. 2024].

²⁴ Segundo o artigo 3º n.º 1 al. rr) da lei n.º 16/2022 de 16 de agosto – Lei das Comunicações Eletrónicas o “«Serviço de comunicações de voz», um serviço de comunicações eletrónicas acessível ao público para efetuar e receber, direta ou indiretamente, chamadas nacionais, ou nacionais e internacionais, através de um número ou de números incluídos em planos nacionais ou internacionais de numeração.”

Quando acedemos à Internet, por exemplo, em casa, a rede é o nosso ISP (Internet Service Provider), e este servidor vai atribuir o endereço IP²⁵ (Internet Protocol) ao dispositivo em utilização, ou seja, a nossa atividade na Internet vai passar pelo ISP e volta para nós, com um endereço IP²⁶.

Com a evolução da tecnologia, a Internet tem mudado muito a forma como nos comunicamos, pois, o e-mail foi considerado o meio de comunicação mais rápido há alguns anos, mas, atualmente, o mesmo já não é considerado rápido o suficiente e, com isto, surgiu os chamados aplicativos OTT (Over the top), ou seja, são mensagens instantâneas que consiste em um aplicativo prático de usar que conecta várias pessoas sendo utilizado texto e comunicação visual, em tempo real²⁷ e estão disponíveis para os smartphones, computadores e tablets de forma gratuita, ao contrário das SMS²⁸.

Ora, as principais aplicações são, conversações no Messenger, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagens via WhatsApp, Viber, Skype, Snapchat, Telegram, Facebook, entre outros²⁹.

Contudo, para finalizar este capítulo, é importante referir que todos estes meios de comunicação se aplicam as regras quanto à apreensão do correio eletrónico e de registos de comunicação de natureza semelhante,

Desde que se encontrem armazenados no sistema informático que tenha sido acedido pelas autoridades e não à sua interceção em tempo real, sendo aplicável o regime da apreensão da correspondência, previsto no art.º 179º do CPP, bem como o disposto no art.º 252º do CPP³⁰.

Com a mesma opinião, refere Rui Cardoso, “Porém, por regra, as mensagens transmitidas ficam armazenadas nos sistemas dos intervenientes, podendo, por isso, tais dados ser apreendidos.”³¹.

²⁵ Consiste num identificador que permite que as informações sejam enviadas entre dispositivos conectados a uma rede, o mesmo carrega dados de localização permitindo assim que o dispositivo fique acessível para a comunicação.

²⁶ Kaspersky – Endereço IP. Disponível para consulta em <https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address> [Consult. 30 out. 2024].

²⁷ EZTALKS – Mensagens instantâneas. Disponível par consulta em <https://pt.eztalks.com/unified-communications/8-examples-of-instant-messaging.html> - google vignette, [Consult. 30 out. 2024].

²⁸ TWILIO – Mensagens. Disponível para consulta em <https://www.twilio.com/pt-br/learn/messaging/what-are-sms-and-mms> [Consult. 4 nov. 2024].

²⁹ Nunes, Duarte Rodrigues, ob. cit., p. 332.

³⁰ Idem, pp. 333 e 334

³¹ Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX, p. 69, [Consult. 30 out. 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>. ISBN 978-989-8908-17-9.

Isto porque, alguns criminosos que estejam em sítios diferentes e queiram comunicar entre si, utilizam estes meios de comunicação, anteriormente, analisados, devido à sua rapidez, sem ser preciso se encontrarem pessoalmente³², e há outros indivíduos que utilizam estas redes sociais para práticas ilícitas, como por exemplo, pornografia infantil³³, onde estes partilham e descarregam imagens e vídeos de crianças, ou as situações de criminalidade violenta ou altamente organizada.

Nestes casos, é importante a leitura de um email ou de outro registo de comunicação de natureza semelhante pelas autoridades competentes, para que se possa obter uma resposta investigatória, que poderá levar a um resgate ou até mesmo descobrir/encontrar o criminoso.

³² Nunes, Duarte Rodrigues, (2021), p. 332.

³³ Crime previsto e punido pelo artigo 176.º do Código Penal Português.

Capítulo 2: Evolução do tratamento legislativo da apreensão de correio eletrónico e registos de comunicação de natureza semelhante

1. Código Processo Penal antes de 2009

Em 1998, com as alterações introduzidas pela Lei n.º 59/98, de 25 de agosto no CPP, o correio eletrónico passa a ser um meio de obtenção de prova equiparado ao telefone, ou seja, para além dos exames, das revistas, das buscas e das apreensões, “(...) encontram-se no Código de Processo Penal outros meios de obtenção e produção de prova no decurso de uma investigação criminal, que têm por objecto os telefones, os telemóveis, o correio electrónico, entre outros meios de comunicação.”³⁴.

No ano de 2007, quando o Código de Processo Penal foi revisto pela Lei n.º 48/2007, de 29 de agosto, veio alterar os artigos 189.º e 190.º do referido diploma, passando o artigo 189.º a realizar a extensão do regime das escutas telefónicas a outras formas de comunicação e o artigo 190.º a prever o efeito da nulidade no caso de violação dos artigos 187.º, 188.º e 189.º³⁵.

Ora, o artigo 189.º do mesmo diploma, passou a ter uma referência relativamente à interceção do correio eletrónico e das outras formas de transmissão de dados por via telemática mesmo estando guardas em suporte digital³⁶, já os artigos 187.º e 188.º do CPP (interceção de comunicações), consagram a interceção de uma comunicação em tempo real e com a devida autorização do JIC para se proceder à sua apreensão.

O correio eletrónico não tinha um regime específico, o que fez gerar divergências na doutrina e na jurisprudência, pois, não era claro qual as regras que o correio eletrónico deveria seguir, ou seja, as regras da interceção de comunicações presente nos artigos 187.º e 188.º do CPP ou as regras da apreensão de correspondência (art. 179.º do CPP), no entanto, este será um tema que vamos estudar mais à frente, neste trabalho.

Em 2009, após a entrada em vigor do texto reviso do Código Processo Penal, o nosso legislador, veio consagrar novas normas processuais e penais relevantes em matéria de prova eletrónica, ou seja, a Lei n.º 32/2008, de 17 de julho³⁷, que visou transpor para a

³⁴ Neves, Rita Castanheira, ob. cit., p. 142.

³⁵ Idem, pp. 140 e 141.

³⁶ Idem, *ibidem*.

³⁷ Foi atualizada pela Lei n.º 18/2024, de 5 de fevereiro.

ordem jurídica interna a Diretiva n.º 2006/24/CE do Parlamento Europeu e do Conselho de 15 de março, que trata sobre a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e, por fim, a Lei n.º 109/2009, de 15 de setembro, resultante das obrigações internacionais do Estado português por força da Decisão-Quadro n.º 2005/222/JAI, de 16 de março de 2005 e da Convenção do Conselho da Europa sobre o Cibercrime³⁸.

Relativamente, à parte da prova eletrónica, a Lei do Cibercrime apenas fez cumprir as do Estado português derivadas da Convenção do Conselho da Europa a respeito da recolha de prova eletrónica preenchendo a lacuna do direito processual penal geral. Ou seja, com esta lei, pretendeu-se dar resposta às limitações presentes na revisão do Código de Processo Penal de 2007, permitindo assim, a obtenção de dados de tráfego e a realização de interceção de comunicações eletrónicas na investigação de crimes não previstos no artigo 187.º do CPP³⁹.

A entrada em vigor da Lei do Cibercrime, nomeadamente o seu artigo 17.º (apreensão de correio eletrónico e de registos de comunicação de natureza semelhante), teve com consequência, a alteração da matriz adotada na redação de 2007 do artigo 189.º n.º 1 do CPP, ou seja, o regime do correio eletrónico dos crimes não referidos no artigo 187.º, deixou de estar sujeito às regras da interceção de telecomunicações, remetendo-se, posteriormente, para o regime da apreensão da correspondência presente no artigo 179.º do CPP, tal como acontece até aos dias de hoje.

2. Diplomas internacionais na base da Lei do Cibercrime (Lei n.º 109/2009 de 15 de setembro)

A Lei do Cibercrime (109/2009, de 15 de setembro), foi criada para combater os desafios gerados pela criminalidade no ciberespaço, no entanto, tem como base legislativa não só no direito interno, mas também a nível internacional e europeu.

Os diplomas mais relevantes para abordar são a Convenção de Budapeste sobre o Cibercrime, a Decisão-Quadro 2005/222/JAI do Conselho da União Europeia, que estabelece as normas contra aos ataques a sistemas de informação, por fim, o

³⁸ Mesquita, Paulo Dá (2010) – Processo Penal, Prova e Sistema Judiciário, 1ª ed., Coimbra Editora, p. 96.

³⁹ Idem, p. 97.

Regulamento Geral sobre a Proteção de Dados, que será abordado de forma breve, dando mais ênfase à Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes durante as investigações.

2.1 Convenção de Budapeste sobre o cibercrime

A evolução das tecnologias da informação e das comunicações alterou radicalmente a forma como as pessoas passaram a comunicar entre si, neste caso, a Internet veio permitir que as pessoas tenham acesso à informação, que se encontra inserida no sistema informático, e que pode ser utilizada em qualquer parte do mundo.

Com isto, as empresas também saíram beneficiadas, porque começaram a centrar a sua atividade económica no ciberespaço, chegando assim a um maior número de consumidores, que conseqüentemente, obtiveram um aumento do lucro⁴⁰.

Relativamente ao surgimento das redes sociais, como já foi referido, potencializou também uma crescente e mais rápida interação entre as pessoas, em qualquer parte do mundo⁴¹.

Contudo, tudo isto apresenta aspetos positivos, mas também aspetos negativos, ou seja, a evolução da tecnologia veio proporcionar às pessoas o uso de novas formas de comunicar para fins lícitos, mas também para fins ilícitos⁴².

Os criminosos ao utilizarem os meios informáticos para sua atividade criminosa, “esses meios permitem apagar as barreiras psicológicas que muitas vezes existe quando um criminoso tem de encarar a vítima e atingir pessoas em todo o Mundo e num número muito mais elevado e dificultam a localização e a identificação do criminoso e a recolha de prova.”⁴³.

⁴⁰ No mesmo sentido, Nunes, Duarte Rodrigues, (2021), p. 11.

⁴¹ Idem, *ibidem*.

⁴² Idem, pp. 12 e 13.

⁴³ Idem, p. 18.

Os crimes que podem ser cometidos por meios informáticos são de variada natureza desde atos terroristas (criminalidade organizada), pornografia infantil⁴⁴, tráfico de armas, seres humanos e órgãos, de droga, homicídios, entre outros.

Tal como refere o Relatório Explicativo da Convenção sobre o Cibercrime:

1. A revolução nas tecnologias da informação operou mudanças fundamentais na sociedade e irá provavelmente continuar a fazê-lo num futuro previsível. Foram inúmeras as tarefas cuja execução se tornou mais fácil.
Enquanto que, inicialmente, apenas alguns sectores específicos da sociedade procederam a uma racionalização dos seus métodos de trabalho, com a ajuda das tecnologias da informação, actualmente, não existe praticamente nenhum sector da sociedade que não tenha sido abrangido pelas mesmas.
As tecnologias da informação vieram, de uma forma ou de outra, conferir novos contornos a quase todos os aspectos das actividades do Homem.
2. Uma característica notável da tecnologia da informação reside no impacto que esta teve, e ainda virá a ter certamente, na evolução da tecnologia das telecomunicações. Os clássicos sistemas telefónicos, envolvendo a transmissão da voz do Homem, foram suplantados por sistemas de permuta de grandes quantidades de dados, incluindo sob a forma de voz, texto e música, assim como de imagens estáticas e móveis.
Esta permuta não se dá apenas entre seres humanos, mas também entre estes os computadores, e ao nível dos sistemas de computadores entre si.
As ligações por comutação de circuitos foram substituídas por ligações por comutação de pacotes.
Nos dias de hoje, já não é importante o facto de se poder ou não estabelecer uma ligação directa; basta que os dados em questão sejam introduzidos numa rede com um endereço de destino ou que sejam disponibilizados a todos quantos desejem aceder-lhes.
3. A utilização universal do correio electrónico e o acesso aos inúmeros *sites* através da Internet constituem o exemplo desses desenvolvimentos que tão profundamente contribuíram para a mudança ocorrida na nossa sociedade.
4. A fácil acessibilidade e pesquisa da informação contida em sistemas informáticos, aliada às possibilidades quase ilimitadas relativamente à sua permuta e difusão, não

⁴⁴ Para consulta, Relatório Explicativo da Convenção do Conselho da Europa para a Proteção das crianças contra a Exploração Sexual e aos Abusos Sexuais (2020) - Lanzarote, 25.X.2007. "A Convenção sobre o Cibercrime (ETS 185, Conselho da Europa, 2001) contempla uma disposição específica, o Artigo 9.º que criminaliza a pornografia infantil quando, para tal, tenha sido utilizado um sistema informático. Contém uma definição de pornografia infantil e convida os Estados Partes a criminalizar a produção, a oferta ou disponibilização, a difusão ou transmissão, a obtenção e a posse de pornografia de menores. As importantes medidas de cooperação processual e internacional contidas nesta Convenção, também se aplicam a outras infrações penais cometidas com recurso a um sistema informático e à recolha de provas, em formato eletrónico, da infração penal (por exemplo, no caso da exploração ou abuso sexual de crianças).", p. 6.

Disponível em https://dgpj.justica.gov.pt/Portals/31/Edi%E7%F5es DGPJ/REL_EXP.pdf.

obstante as distâncias geográficas, traduziu-se por um crescimento explosivo da quantidade de informação disponível e do conhecimento que daí advém.

5. Estes desenvolvimentos deram origem a mutações sociais e económicas sem precedentes, mas apresentam simultaneamente uma faceta negativa: a emergência de novos tipos de criminalidade, bem como a prática dos crimes tradicionais com o recurso às novas tecnologias.

Além disso, as consequências do comportamento de índole criminosa poderão ser mais extensas e ter um maior alcance uma vez que não estão restringidas por quaisquer limites geográficos ou fronteiras nacionais.

A recente disseminação de vírus informáticos prejudiciais, um pouco por todo o mundo, comprova esta realidade.

As medidas de carácter técnico que visam proteger os sistemas informáticos deverão, pois, ser tomadas concomitantemente com medidas de natureza jurídica a fim de evitar e deter a prática de crimes.⁴⁵.

Ora, o Conselho da Europa⁴⁶ (instituição da União Europeia) como estava ciente desta realidade, criou diversas diligências com a finalidade de incrementar a resposta ao cibercrime, surgiu assim a Convenção sobre o Cibercrime do Conselho da Europa, onde esta tem como objetivo principal “(1) a harmonização dos elementos relativos a infracções no contexto do direito penal substantivo de âmbito nacional e das disposições conexas na área da cibercriminalidade, (2) a definição, ao abrigo do processo penal interno, dos poderes necessários para investigar e intentar acções penais relativamente a tais infracções cometidas por meio de um sistema informático ou às provas com elas relacionadas e existentes sob a forma electrónica, (3) a implantação de um regime rápido e eficaz de cooperação internacional.”⁴⁷.

A Convenção está dividida em quatro capítulos, o primeiro deve-se à utilização de terminologia; o segundo capítulo insere-se nas medidas a empreender ao nível nacional - direito substantivo e direito processual; o terceiro consiste na cooperação internacional, e por fim, o quarto capítulo inclui as disposições finais.

A referida Convenção foi aberta à assinatura em Budapeste, em 23 de novembro de 2001, sendo que em Portugal também foi assinada nesta data, no entanto, foi também aprovada pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro, e ratificada pelo Decreto do Presidente da República n.º 91/2009, de 15 de setembro⁴⁸.

⁴⁵ Minuta de Relatório Explicativo, disponível em <https://rm.coe.int/16802fa429>.

⁴⁶ Artigos 235.º e 236.º do TFUE.

⁴⁷ Minuta de Relatório Explicativo, disponível em <https://rm.coe.int/16802fa429>.

⁴⁸ Ministério Público – Consulta de tratados internacionais. Convenção sobre o Cibercrime. Disponível em <https://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0>.

2.2 Decisão-Quadro 2005/222/JAI do Conselho da União Europeia

Com a evolução da tecnologia e com a desatualização da Lei da Criminalidade Informática, surgiu a necessidade de modernizar o quadro legal.

Nesse contexto, a Lei n.º 109/2009, de 15 de setembro, aprovou a Lei do Cibercrime, que transpôs para a ordem jurídica interna a referida Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro e adaptou o direito interno às disposições da Convenção sobre o Cibercrime, que foi adotada em Budapeste em 23 de novembro de 2001 no âmbito do Conselho da Europa, que entrou em vigor na ordem internacional a 1 de julho de 2004⁴⁹.

A Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, tem como objetivo “reforçar a cooperação entre as autoridades judiciais e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação.”⁵⁰.

Esta Decisão-Quadro, limita-se aos crimes de acesso ilegal aos sistemas de informação previsto no seu artigo 2.º, a interferência ilegal no sistema (artigo 3.º) e à interferência ilegal de dados, que está presente no artigo 5.º, no entanto, não apresenta meios processuais específicos para a obtenção de prova digital, ao contrário do que acontece na Convenção de Budapeste⁵¹.

Porém, a Decisão-Quadro n.º 2005/22/JAI foi substituída pela Diretiva n.º 2013/40/EU do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, que trata sobre os ataques contra os sistemas de informação, mas não existiu nenhuma alteração na Lei do Cibercrime por parte do nosso legislador, o que dá a entender que a mesma não precisava de ser alterada⁵².

Para finalizar, a Lei do Cibercrime teve a sua primeira alteração pela Lei n.º 79/2021, de 24 de novembro, que transpõe a Diretiva (UE) 2019/713 do Parlamento Europeu e do

⁴⁹ Ministério Público – Consulta de tratados internacionais. Convenção sobre o Cibercrime. Disponível em <https://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0>.

⁵⁰ Jornal Oficial da União Europeia. Disponível em <https://op.europa.eu/pt/publication-detail/-/publication/708d86d8-ab9a-4e18-9bda-ac37405a3185>.

⁵¹ Venâncio, Pedro Dias, ob. cit., p. 25.

⁵² Idem, p. 26.

Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, alterando assim também o Código Penal, o Código Processo Penal e outros atos legislativos⁵³.

2.3 Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016

O regime da proteção de dados pessoais está contemplado no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD) que regula o regime relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (entrou em vigor desde o dia 25 de maio de 2018), e pela Lei n.º 58/2019, de 8 de agosto que assegura a execução na ordem jurídica interna do referido regulamento.

O Regulamento da RGPD, visa proteger todos os cidadãos da UE contra violações da privacidade e dos dados num mundo baseado em dados⁵⁴, ou seja, estabelece direitos fundamentais das pessoas na era digital; aplica sanções aos criminosos, refere métodos para assegurar o cumprimento e, por fim, indica as obrigações dos responsáveis pelo tratamento de dados⁵⁵.

No entanto, numa investigação penal, o tratamento de dados pessoais é regulado pelo regime previsto da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, pelo que em Portugal a referida lei foi transposta para o direito interno pela Lei n.º 59/2019,

⁵³ Ministério Público - Procuradoria-Geral Regional de Lisboa. Lei n.º 79/2021, de 24 de novembro. Para consulta, disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3476&tabela=leis&ficha=1&pagina=1&so_mio_lo=-.

⁵⁴ Fichas temáticas sobre a União Europeia – 2025, disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf.

⁵⁵ Conselho Europeu/Conselho da União Europeia (2024) – Regulamento Geral Sobre a Proteção de Dados, [Consult. 15 jan. 2025]. Disponível em <https://www.consilium.europa.eu/pt/policies/data-protection/data-protection-regulation/>.

de 8 de agosto (Dados Pessoais para Prevenção, Detecção, Investigação ou Repressão de Infrações Penais).

A diretiva protege o direito fundamental dos cidadãos à proteção de dados quando os dados pessoais forem utilizados pelas autoridades responsáveis pela aplicação da lei. Garante ainda que os dados pessoais das vítimas, testemunhas e suspeitos de crimes sejam devidamente protegidos e facilita a cooperação transfronteiriça na luta contra a criminalidade e o terrorismo⁵⁶.

Porém, o artigo 30.º da Lei do Cibercrime, teve uma alteração promovida pela Lei n.º 79/2021, de 24 de novembro que se baseia na atualização da Lei de Proteção de Dados em matéria de investigação vigente em Portugal, em que substituiu a Lei n.º 67/98, de 26 de outubro, pela lei 59/2019, de 8 de agosto, no entanto, o referido artigo remete para os capítulos VII, referente aos meios de tutela e responsabilidade e ao capítulo VIII que faz referência às sanções da última lei referida⁵⁷.

Isto significa que, caso aconteça uma violação de dados pessoais no âmbito de uma investigação penal que envolva prova digital, deve-se aplicar os crimes previstos na Lei n.º 59/2019, de 8 de agosto e não aqueles previstos na Lei n.º 58/2019, de 8 de agosto que regula o RGPD em geral.

Exposto isto, seguiremos para o terceiro capítulo, onde vamos estudar a fundo o tema deste trabalho, neste caso, o artigo 17.º da Lei do Cibercrime (Apreensão de correio eletrónico e registos de comunicações de natureza semelhante).

⁵⁶ Fichas temáticas sobre a União Europeia – 2025, disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf.

⁵⁷ Venâncio, Pedro Dias, ob. cit., p. 235.

Capítulo 3: Análise do artigo 17º da Lei do Cibercrime

1. Generalidades

Antes de começarmos a analisar o tema mais pertinente deste trabalho, vamos perceber em que consiste o conceito de cibercrime e o qual é o conceito dado pela nossa doutrina.

Para começarmos importa referir que há mais do que um conceito de cibercrime.

Consideramos que o conceito de cibercrime em sentido amplo consiste num facto tipificado como crime que é praticado através de um sistema informático, ou seja, em qualquer dispositivo (artigo 2.º, al. a), da Lei do Cibercrime), explicando por outras palavras, pode-se falar em cibercrime em sentido amplo sempre que o agente do crime utilize a Internet para cometer um ato ilícito que, neste caso, poderia ser praticado sem a utilização de um sistema informático, como por exemplo, os crimes de ódio e difamação ou o tráfico de drogas.

Em sentido estrito, o conceito de cibercrime trata-se de crimes praticados no sistema informático, ou seja, os criminosos têm como alvo atacar a segurança cibernética e/ou a integridade dos dados (ex.: burla informática e os crimes previstos na Lei n.º 109/2009), ou seja, estes tipos de crimes dependem da utilização da Internet e são contra a sua segurança.

Relativamente à nossa doutrina, a perspetiva do autor Pedro Dias Venâncio, aponta que

Em sentido amplo, então, a criminalidade informática englobará toda a panóplia de actividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios.

Em sentido estrito, entenderemos nós que a criminalidade informática abarcará apenas aqueles crimes em que o elemento digital surge como parte integradora do tipo legal ou mesmo como seu objecto de protecção⁵⁸.

O mesmo autor acaba por adotar o conceito em sentido estrito⁵⁹.

Já o autor Pedro Verdelho tem uma visão tripartida dos crimes a propósito do cibercrime,

⁵⁸ Nunes, Duarte Rodrigues, (2021), pp. 37 e 38, *apud* Venâncio, Pedro Dias (2011) - Lei do Cibercrime, Anotada e Comentada, Coimbra Editora, p. 17; com mesma opinião, Freitas, José Pedro, ob. cit., pp. 62 e 63.

⁵⁹ *Idem*, p. 38.

É, porém, incontornável reconhecer que as realidades sociológicas de tipo criminógeno actualmente discutidas a propósito do cibercrime estão muito para lá daquilo que na lei portuguesa se consagrou como “criminalidade informática”.

Por um lado, existem crimes cometidos por via de computadores ou sistemas de computadores que, não obstante o meio pelo qual são cometidos, não se distinguem do mesmo tipo de crime cometido por outras vias.

Embora sejam crimes cometidos on-line, isso não lhes confere nenhuma especialidade. Dogmaticamente nada os distingue da sua forma tradicional, apenas tendo de diferente o meio usado (...).

Destes se distinguem outros crimes, que têm de especial o ambiente em que são praticados.

Não poderiam ser cometidos noutro meio nem por outro meio.

São gerados no ambiente informático e só podem ocorrer pela especificidade do meio (...).

Mas ainda há uma outra espécie de crimes, os quais se caracterizam por serem praticados contra o meio informático.

São crimes contra computadores ou sistemas de computadores.

São os crimes informáticos propriamente ditos (...).

Deste conjunto inorgânico, no fundo, importa reter que o que está em causa são os crimes relacionados com a utilização de computadores, com particular incidência naqueles que estão ligados a redes informáticas e, em especial, à Internet⁶⁰.

Segundo a Comissão Europeia, o cibercrime consiste em “atos criminosos cometidos utilizando redes de comunicações eletrónicas e sistemas de informação ou contra essas redes e sistemas.”⁶¹, ou seja, o conceito de cibercrime, aplica-se aos três tipos de atividade criminosa referida por Pedro Verdelho.

A primeira insere-se nas formas tradicionais da criminalidade, como a fraude e a falsificação, que acontecem nos sistemas de informação e em redes de comunicação eletrónicas, já a segunda abrange as publicações de conteúdos ilícitos, tais como pornografia infantil, incitamento ao ódio racial, entre outros; por fim, temos a terceira atividade criminosa que refere-se a crimes exclusivos das redes eletrónicas, ou seja, quando os criminosos atacam sistemas de informação e estes ataques podem ser contra a infraestruturas de informação cruciais do Estado, causando assim consequências desastrosas para a sociedade⁶².

⁶⁰ Idem, pp. 38 e 39, *apud* Verdelho, Pedro “Cibercrime”, in *Direito da Sociedade da Informação*, IV, pp. 347-348.

⁶¹ Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões (2015) - Rumo a uma política geral de luta contra o cibercrime, [Consult. 4 de jan. 2025]. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3A14560&qid=1736473558179>.

⁶² Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões (2015) - Rumo a uma política geral de luta contra o cibercrime, [Consult. 4 jan. 2025]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3A14560&qid=1736473558179>.

Ora, estas três categorias de atividade criminosa, podem ser praticadas em grande escala e por todo o mundo, podendo, deste modo, o criminoso estar num determinado país e os efeitos da sua atividade ilícita ser num país diferente⁶³.

Exposto isto, entendemos que o conceito de cibercrime não deve ser demasiado restrito, pois deixaria de parte algumas condutas que exigem mecanismos específicos típicos do combate ao cibercrime, sem estes mecanismos previstos na lei, tornar-se-ia difícil haver proteção jurídica e as autoridades competentes não terão meios de prevenção eficazes⁶⁴.

Temos como exemplo prático, desta situação, crime de pornografia infantil praticado através da Internet.

Se não fosse consagrado a obtenção de dados de tráfego armazenados que abrangem as comunicações anteriormente efetuadas, não seria possível saber a origem/destino de uma comunicação que permitisse identificar a pessoa, que, por exemplo, partilhava essa pornografia infantil ou espalhava declarações falsas no contexto de uma operação fraudulenta (ex.: Phishing⁶⁵).

Estes dois crimes não são crimes contra os sistemas informáticos, mas sim, contra pessoas, os criminosos usam apenas a Internet como meio para praticar o ato ilícito.

Também entendemos que o conceito de cibercrime em sentido amplo também não pode ser demasiado amplo, porque pode abarcar comportamentos ou situações que não devam ser considerados como crimes informáticos, consequentemente, poderá levar à aplicação de mecanismos específicos de forma desproporcional e desnecessária⁶⁶.

Ademais, faz cada vez menos sentido diferenciar o plano do Direito penal material do plano do Direito processual penal, razão pela qual, a delimitação do conceito de cibercrime deverá ter em conta, por um lado, a determinação das condutas criminosas que devam ser incluídas no âmbito da criminalidade informática e, por outro, a determinação das condutas criminosas relativamente às quais se mostre necessário lançar mão de meios investigatórios para obtenção de prova digital⁶⁷.

Após esta explicação, seguiremos para análise da nossa Lei do Cibercrime.

⁶³ No mesmo sentido, Nunes, Duarte Rodrigues, (2021), p. 42.

⁶⁴ Idem, p. 43.

⁶⁵ É um crime cibernético em que os criminosos tentam obter informações confidenciais das pessoas, enviando emails com links fraudulentos para que as mesmas abram e preencham formulários com as suas informações pessoais. Para consulta, Malwarebytes – Phishing. Disponível em <https://www.malwarebytes.com/pt-br/phishing>.

⁶⁶ No mesmo sentido, Nunes, Duarte Rodrigues, (2021), p. 44.

⁶⁷ Idem, *ibidem*.

No ordenamento jurídico português já vigorava desde 1991 a “Lei da Cibercriminalidade Informática” (109/91, de 17 de Agosto)⁶⁸, este diploma, que contava com 19 artigos, regulou a matéria sobre o cibercrime, apresentando assim, o catálogo de crimes ligados à informática, as penas acessórias e, ainda, a responsabilidade criminal das pessoas coletivas⁶⁹.

A Lei do Cibercrime surge como um diploma fundamental para o combate à criminalidade no âmbito da Internet.

Esta Lei assume a estrutura da Convenção de Budapeste, dividindo-se em 4 capítulos, ou seja, no primeiro é apresentado o “Objeto e Definições”, no segundo temos as “Disposições Penais Materiais”, no terceiro capítulo surgem as “Disposições Processuais” e, por fim, o quarto dispõe a “Cooperação Internacional”⁷⁰.

Ora, o artigo 17.º da Lei do Cibercrime, trata-se de uma inovação do legislador português, porque o artigo 19.º da Convenção do Budapeste não refere, expressamente, a apreensão de mensagens de correio eletrónico, mas se prestarmos atenção ao ponto 190 da Convenção, o legislador internacional deixou ao critério do legislador nacional a opção de lhe consagrar ou não um regime especial⁷¹.

Nesta lei, existem diversos meios de obtenção de prova que permitem à entidade competente, pela investigação, que tenha conhecimento do conteúdo das comunicações realizadas, como acontece com o artigo 17.º, que consiste na apreensão do correio eletrónico e de registos de comunicação de natureza semelhante e o artigo 18.º que consagra a interceção de comunicações.

A diferença nestes dois últimos artigos referidos, deve-se ao facto, de que no primeiro artigo, a obtenção da prova será quando o processo comunicacional tenha terminado, enquanto, que no artigo 18.º a obtenção da prova acontece em tempo real, ou seja, no decorrer do processo comunicacional⁷².

⁶⁸ Carvalho, Francisco Proença De, Óscar Morales Garcia e Manuel Álvarez Feijoo (2018) - Regulamentação Supranacional sobre a Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como paradigmas, n.º 48, p. 53 [Consult. 10 nov. 2024]. Disponível em <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877> ISSN: 1578-956X.

⁶⁹ Freitas, José Pedro, ob. cit., p. 68.

⁷⁰ Carvalho, Francisco Proença De, Óscar Morales Garcia e Manuel Álvarez Feijoo (2018) - Regulamentação Supranacional sobre a Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como paradigmas, n.º 48, p. 54 [Consult. 10 nov. 2024]. Disponível em <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877> ISSN:1578-956X.

⁷¹ Venâncio, Pedro Dias, ob. cit., p. 181.

⁷² Nunes, Duarte Rodrigues, (2021), pp. 332 e 333.

Ora, focando precisamente no artigo 17.º, este dispõe que *“quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutra a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico 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 de apreensão de correspondência previsto no Código de Processo Penal.”*

Exposto isto, entendemos que quando o juiz autorizar ou ordenar, por despacho, a apreensão do correio eletrónico e/ou os registos de comunicação de natureza semelhante, desde logo, os que foram referidos no primeiro capítulo (SMS, MMS, EMS, conversações no Messenger, mensagens de voz relativas a comunicações ou arquivos de som e/ vídeos por via WhatsApp, Viber, Skype, Snapchat, Telegram e Facebook), estes têm de estar armazenados no sistema informático para que a entidade competente, após a autorização do juiz, possa obter a informação que contenha um grande interesse para a descoberta da verdade material⁷³ ou para a prova, porém, a distinção entre as comunicações em tempo real e as comunicações já armazenadas, revelam a preocupação do legislador em tratar com proporcionalidade os diferentes momentos da comunicação, garantindo, assim, um equilíbrio entre a realização da investigação criminal e o respeito pelos direitos fundamentais.

Neste processo, a Lei especial do Cibercrime, no artigo 17.º, remete para o regime de apreensão de correspondência previsto no Código de Processo Penal, nomeadamente, no artigo 179.º.

Este tema será tratado posteriormente, sendo previamente considerado importante identificar quais crimes se enquadram neste regime.

2. Lista de crimes que permitem a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante

⁷³ Princípio da investigação: consiste no Tribunal ter o poder e o dever de investigar os factos sujeitos a julgamento indo para além dos contributos que as partes trazem para o processo, de modo que seja possível encontrar a verdade material dos factos e obter uma decisão mais justa no âmbito do processo penal.

Nesta parte do estudo, vamos analisar quais os crimes que permitem a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante.

Começaremos por abordar a Lei do Cibercrime, ou seja, o seu artigo 17.º, como sabemos, remete para o artigo 179.º do CPP, que refere no seu n.º 1, al. b) “*Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos*”, com isto, entendemos que está presente uma restrição ao recurso à apreensão de correspondência à investigação de crimes puníveis com pena de prisão superior a 3 anos⁷⁴.

Esta remissão resulta da conjugação do artigo 17.º com o artigo 11.º, n.º 1 (âmbito de aplicação das disposições processuais), ambos da Lei do Cibercrime.

Estas disposições processuais presentes na Lei do Cibercrime resultam da transposição para o direito interno das medidas de direito processual previstas na Convenção da Budapeste, que estão estabelecidas no seu artigo 14º⁷⁵.

No artigo 11.º, n.º 1, al. a) da Lei do Cibercrime, não apresenta grandes dúvidas em relação à aplicação dos crimes informáticos previstos na referida lei⁷⁶, mas a al. b) estabelece que as medidas relativas à apreensão de dados informativos (tendo em conta apenas o artigo 17.º) se destinam não só a crimes informáticos que estão previstos na referida lei, mas também a todos os que sejam “cometidos por meio de um sistema informático”⁷⁷, já na al. c) acrescenta ainda que as medidas processuais consagradas, que se aplicam a diversos crimes “em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico”⁷⁸.

A Lei n.º 109/2009, de 15 de setembro, como foi possível ver, tem uma relação estreita com o modelo processual do Código Processual Penal, mas não dispõe de todos os tipos de crimes informáticos presentes na Convenção de Budapeste, ou seja, os demais ilícitos penais estão espalhados pela legislação avulsa e pelo Código Penal⁷⁹ que dispõe de alguns, tais como, a pornografia de menores (art.º 176.º), a devassa através de meio de comunicação social, da internet ou de outros meios de difusão pública generalizada

⁷⁴ Nuno, Rodrigues Duarte, (2021), p. 351.

⁷⁵ Venâncio, Pedro Dias, ob. cit., p. 123.

⁷⁶ Mesquita, Paulo Dá, ob. cit., p. 108.

⁷⁷ Idem, pp. 108 e 109.

⁷⁸ Idem, pp. 109 e 110.

⁷⁹ Venâncio, Pedro Dias, ob. cit., p. 23.

(art.º 193.º), violação de correspondência (art.º 194.º), e a burla informática e nas comunicações (art.º 221.º)⁸⁰.

Exposto isto, percebemos que não existe qualquer lista de crimes para o regime da apreensão de correio eletrónico e de registos de comunicação de natureza semelhante, logo, como refere Paulo Mesquita, “pelo que as regras processuais são aplicáveis de uma forma geral a um universo de crimes aberto, independente dos elementos típicos.”⁸¹.

Seguiremos para o próximo ponto deste trabalho, mais precisamente, a referida remissão do artigo 17.º da Lei do Cibercrime para o regime da apreensão de correspondência, previsto no artigo 179.º do CPP.

3. Remissão para o artigo 179º do CPP

O nosso CPP atual, tem a sua génese no Decreto de Lei n.º 78/87, de 17 de fevereiro, mas até hoje tem sofrido diversas alterações legislativas⁸², uma delas recaiu sobre a prova digital.

Com a evolução tecnologia, a prova digital é um tema que passou a estar integrado no nosso ordenamento jurídico.

Considerando que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, faz referência ao artigo 179.º do Código de Processo Penal (Apreensão de Correspondência), entende-se que o legislador procurou adaptar as disposições relativas à busca e apreensão às novas realidades, sem, contudo, determinar a sua aplicação integral^{83 84}.

⁸⁰ Carvalho, Francisco Proença De, Óscar Morales Garcia e Manuel Álvarez Feijoo (2018) - Regulamentação Supranacional sobre a Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como paradigmas, n.º 48, p. 54 [Consult. 12 nov. 2024]. Disponível em <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877> ISSN:1578-956X.

⁸¹ Mesquita, Paulo Dá, ob. cit., p. 98.

⁸² Neves, Rita Castanheira, ob. cit., p. 137.

⁸³ Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX, p. 74, [Consult. 6 dez. 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

⁸⁴ No mesmo sentido Acórdão TRL de 10-08-2020, proc. 6330/18.8JFLSB-A.L1-3, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8ce57ecb0a16a8e0802585ec0036019a?OpenDocument>.

No entanto, essa remissão não permite que o regime da correspondência contrarie a Lei do Cibercrime⁸⁵.

Assim, o artigo 179.º do CPP, refere que:

- 1- Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que:
 - 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 três anos; e
 - c) A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova.
- 2- É proibida, sob pena de nulidade, a apreensão e qualquer outra forma de controle da correspondência entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime.
- 3- O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida.
Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ela ser utilizada como meio de prova, e fica ligado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova.

Esta remissão leva a várias questões relacionadas com o âmbito de aplicação do artigo 17.º da Lei do Cibercrime.

Desde logo o âmbito objetivo do artigo 179.º do CPP é a correspondência ainda em trânsito ou ainda não aberta pelo destinatário, já na Lei do Cibercrime, as mensagens de correio eletrónico ou de registo de comunicações de natureza semelhante podem ser apreendidas independentemente de estarem abertas/lidas ou fechadas/não lidas⁸⁶.

Também importa notar que a al. a) do n.º 1, do artigo 179.º do CPP, a correspondência tem de ser expedida pelo suspeito/arguido⁸⁷ ou lhe ser dirigida, mesmo que sob nome

⁸⁵ Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX, p. 74, [Consult. 6 dez 2024].

Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

⁸⁶ Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX, p. 74, [Consult. 6 dez. 2024].

Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

⁸⁷ Correia, João Conde, et. al. (2020) - Comentário Judiciário do Código Processual Penal, Tomo II, Artigos 124º a 190º, 2ª ed., Almedina Editora, pp. 644 e 645.

diverso ou através de pessoa diversa, sendo que na Lei n.º 109/2009, de 15 de setembro, não existe qualquer restrição, ou seja, pode ser qualquer pessoa⁸⁸.

Relativamente à al. b) do n.º 1 do artigo anteriormente referido, a apreensão de correspondência só vale como meio de prova para crimes puníveis “com pena de prisão superior, no seu máximo, a três anos”, enquanto, no artigo 17.º da Lei do Cibercrime, não existe catálogo de crimes por força do artigo 11.º do mesmo diploma, como já tínhamos analisado no subtítulo anterior.

Observa-se que tanto o artigo 179.º do CPP quanto a Lei do Cibercrime adotam o critério da necessidade para a produção de prova, fundamentando-se no requisito de “grande interesse para a descoberta da verdade ou para a prova”.

O que consta no n.º 2, do artigo 179.º do CPP, o artigo 17.º da Lei do Cibercrime não faz qualquer referência, por isso, este último deve operar de acordo com o que está na norma do artigo referido do CPP⁸⁹.

Quanto ao n.º 3 do artigo 179.º do CPP, vamos analisar no subcapítulo seguinte, porque este tema merece um estudo mais aprofundado.

Quanto à remissão do artigo 17.º da Lei do Cibercrime para o regime previsto no artigo 179.º do CPP, importa ressaltar, como já foi referido, que a correspondência deste último artigo tem de se encontrar em trânsito, ou seja, em tempo real, o que acontece diversamente do regime da apreensão do correio eletrónico e registos de comunicações de natureza semelhante, em que a comunicação tem de estar armazenada no sistema informático para ser legitimamente acedido pelas autoridades competentes, não existindo assim qualquer violação ao direito à inviolabilidade da correspondência e de outros meios de comunicação privada ao abrigo do artigo 34.º da CRP⁹⁰.

Talvez por isso alguns autores, como é o caso do autor Duarte Nunes, referem que de *iure condendo* é desnecessária a remissão do artigo 17.º para o artigo 179.º por algumas razões que vamos descrever.

Uma das razões consiste em afirmar que a apreensão de correspondência que está prevista no CPP, configura a retirada do circuito normal do correio impedindo assim que

⁸⁸ No mesmo sentido, Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX, p. 74, [Consult. 6 dez. 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>, contra Venâncio, Pedro Dias, ob. cit., p. 183.

⁸⁹ No mesmo sentido de Neves, Rita Castanheira, ob. cit., p. 274.

⁹⁰ No mesmo sentido, Nunes, Duarte Rodrigues, (2021), p. 336.

a comunicação chegue ao seu destinatário, “pelo que restringe o direito à inviolabilidade da correspondência”, mas quando a apreensão da correspondência que ainda não foi enviada pelo remetente, o processo comunicacional ainda não se iniciou e, por isso, não há proteção do direito à inviolabilidade da correspondência, ou seja, o mesmo acontece quando o destinatário já recebeu a correspondência⁹¹.

Já no caso do correio eletrónico já recebido e armazenado no sistema informático é legitimamente acedido pelas autoridades, daí que apenas se restrinja o direito à intimidade/privacidade, à palavra virtual e à autodeterminação informacional, mas não ao direito à inviolabilidade das comunicações⁹², porque o processo comunicacional já terminou⁹³.

Outra razão, consiste no regime da apreensão da correspondência haver a divisão da correspondência física aberta e lida e o correio eletrónico recebido e lido pelo seu destinatário, porque, assim sendo, a primeira depois de recebida passa a ser um mero documento e fica sujeita à apreensão nos termos gerais, enquanto o correio eletrónico permanece sujeito ao regime da apreensão de correspondência quer seja aberto ou fechado⁹⁴.

Duarte Nunes aponta outra razão para não haver esta remissão que se baseia na dificuldade gerada durante as investigações por causa da opção do legislador, sendo que o objetivo da Lei n.º 109/2009 era facilitar a investigação do cibercrime. Ora tendo em conta o artigo 179.º do CPP, torna-se difícil a sua aplicação no que concerne à abertura e tomada de conhecimento do conteúdo das comunicações, podendo existir vários emails e apenas alguns serem relevantes para a investigação, o que gera um grande esforço por parte do juiz em fazer a abertura prévia, leitura e depois selecionar os que servem como meio de prova. Se tal ocorresse durante a fase de inquérito, os investigadores teriam um melhor conhecimento do que o JIC⁹⁵.

Por fim, a última razão apontada, deve se ao facto, do correio eletrónico, ter um método de abertura diverso da correspondência “tradicional”, ou seja, “(...) a abertura de um e-

⁹¹ Idem, p. 338.

⁹² O direito à inviolabilidade das comunicações consiste numa garantia fundamental, que assegura a proibição na ingerência na correspondência, nas telecomunicações e nos demais meios de comunicação privados dos cidadãos, ou seja, que não sejam violadas por terceiros, salvo nos casos previstos na lei em matéria de processo penal. Cfr. Canotilho, José Joaquim Gomes e Vital Moreira (2007) – Constituição da República Portuguesa, Anotada, volume I, 4ª ed., Coimbra Editora, p. 543.

⁹³ Nunes, Duarte Rodrigues, (2021), pp. 339 e 340.

⁹⁴ Idem, pp. 340 e 341.

⁹⁵ Idem, pp. 341 e 342.

mail nada tem a ver com a abertura de um sobrescrito contendo uma carta e a cifra nada tem a ver com um envelope ou outro invólucro corpóreo, (...).⁹⁶.⁹⁷.

No mesmo sentido, a autora Rita Neves, acrescenta como razão o facto de a correspondência tradicional tem como proteção as comunicações, os riscos de ingerências de terceiros, ou seja, as pessoas que levam as cartas ao respetivo destinatário e deixam as mesmas na caixa de correio, o domínio sobre a correspondência já não está na esfera dos serviços postais públicos, mas sim do destinatário, diversamente, o correio eletrónico, mesmo quando recebido no dispositivo do destinatário, continua acessível de igual forma aos serviços de comunicações eletrónicas⁹⁸.

Para reforçar a posição destes autores podemos referir outras diferenças entre a correspondência física e o correio eletrónico.

Relativamente ao correio eletrónico podemos acrescentar que este nunca está fechado, ao contrário do que acontece com a correspondência por carta, e por não estar em trânsito e de se armazenar num sistema informático ou até mesmo ser destruído é que não pode ser caracterizado por correio em sentido tradicional. Ou seja, a sua natureza imaterial torna o diferente da correspondência por carta, e nem a sua destruição (ser apagado) significa destruição permanente, como acontece com uma carta⁹⁹.

Se tivermos em atenção o conceito de correio eletrónico, segundo a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002¹⁰⁰, nada nos diz sobre o conceito de correspondência, o que demonstra que não existe aqui qualquer equiparação à correspondência tradicional.

Considerando estes dados podemos perceber que o tratamento do ponto de vista legal, deve ser diferente para o correio eletrónico e a correspondência tradicional.

⁹⁶ Idem, pp. 342 e 343.

⁹⁷ O correio eletrónico já recebido é diferente dos outros dados informáticos, como, por exemplo, da folha de cálculo ou um programa para criação ou apresentação digital de slides, que, neste caso, são apreendidos ao abrigo do artigo 16º da Lei do Cibercrime, e que poderão conter informações de cariz privado e íntimo, mas o MP pode autorizar a “apreensão de correspondência ou de uma cópia em suporte papel de um email guardado num cofre e ser necessária a autorização do JIC para se apreender um email guardado num computador. – Idem, pp. 336 e 337.

⁹⁸ Neves, Rita Castanheira, ob. cit., p. 187.

⁹⁹ Bravo, Rogério (2006) - Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta. Revista Polícia e Justiça, Instituto Superior de Polícia Judiciária e de Ciências Criminais III Série, n.º 7, Coimbra Editora, p. 5.

¹⁰⁰ Artigo 2.º al. h) “Correio eletrónico” - “qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário a recolher.”

Vejamos, o primeiro tem uma natureza imaterial, que é enviado através de uma rede pública, e por essa razão, não há a diferenciação da mensagem aberta ou fechada, já a segunda, tem uma natureza material, por ser palpável ou física e encontra-se fechada até o seu respetivo destinatário abrir e por isso há que distinguir o regime da aberta e da fechada.

Sendo assim, importa ter em consideração, que apesar de o correio eletrónico e a correspondência tradicional terem a mesma tutela constitucional, tal como está prevista no artigo 34.º da CRP, o seu regime jurídico não é idêntico, ou seja, a sua aplicação difere para cada uma das comunicações¹⁰¹.

Daí que o correio eletrónico não se encontra previsto no artigo 179.º do CPP, mas sim noutro diploma (artigo 17.º da Lei do Cibercrime), o que demonstra que não se deve fazer tal equiparação entre aquelas duas formas de comunicação, apesar da remissão do artigo 17.º para o artigo 179.º.¹⁰²

3.1 Competência para autorizar a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante

Antes de começarmos a analisar este tema, temos de entender o que está previsto no artigo 17.º da Lei do Cibercrime.

A norma refere que “(...) 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.”

Importa situar onde esta autorização se pode dar.

¹⁰¹ No mesmo sentido, Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX, pp. 79 e 80, [Consult. 9 dez. 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QG6e-U=&portalid=30>.

¹⁰² Ainda sobre este tema, há quem defenda que tanto o correio eletrónico como a correspondência por carta podem ser eliminadas/arquivadas na mesma forma. Especificamente quanto às mensagens de correio electrónico que tenham sido abertas e impressas em papel, não parece haver qualquer motivo para deixar de dar-lhes, analogicamente, o mesmo tratamento do correio tradicional.

Ou seja, serão meros documentos escritos que podem sem qualquer reserva ser apreendidos no decurso de uma busca. - Verdelho, Pedro (2004) - Apreensão de correio electrónico em Processo Penal. Revista do Ministério Público, ano 25, n.º 100, p. 155. Disponível em https://rmp.smppt.pt/ermp/rmp_100/mobile/index.html - p=74.

Como sabemos, o processo penal pode ser dividido em 4 fases, ou seja, a fase de inquérito, a fase de instrução, a fase de julgamento, e quando necessário a fase do recurso.

No entanto, como a nossa lei divide os crimes em três tipos, ou seja, temos os crimes públicos, os crimes semi-públicos e, por fim, os crimes particulares.

Ora, os primeiros, não é necessário a intervenção da vítima para que o processo decorra, o MP tem competência para avançar com o processo por iniciativa própria, após aquisição da notícia do crime, com o respetivo conhecimento próprio, por intermédio dos OPC ou mediante denúncia, num prazo que não pode exceder 10 dias (art. 241.º e 243.º do CPP), neste caso, o processo pode ocorrer contra a vontade do titular dos interesses ofendidos¹⁰³.

Nos crimes semi-públicos, o processo só se inicia após a apresentação de queixa, por parte da vítima ou pela pessoa com legitimidade para tal (art. 49º, n.º 3 do CPP), só assim é que o MP pode agir (art. 49º, n.º 1 do CPP). Neste caso, pode existir desistência da queixa após a mesma ser realizada.

Nos crimes particulares, o processo só se inicia após a apresentação de uma queixa do ofendido ou por parte de outra pessoa titular do direito de queixa e estas têm de se constituir como assistentes no processo e deduzir uma acusação particular (art. 50º, n.º 1 do CPP), caso contrário, o processo não poderá avançar e o MP não desencadeia oficiosamente, como acontece nos crimes públicos¹⁰⁴.

Na fase de inquérito, compete ao MP dirigir, receber as queixas, as denúncias e as participações e apreciar o seguimento a dar-lhes, segundo o artigo 52.º, n.º 2 do CPP.

Nesta fase ao juiz de instrução criminal como “(...) garante dos direitos fundamentais dos diversos intervenientes no processo penal, (...)”¹⁰⁵ compete-lhe autorizar a apreensão da correspondência, mas é o MP que irá proceder a essa apreensão, ou então, irá delegar aos OPC.

¹⁰³ Para consulta, Ministério Público – Portugal. Disponível em <https://www.ministeriopublico.pt/perguntas-frequentes/crime>.

¹⁰⁴ Para consulta, Diário da República. Disponível em <https://diariodarepublica.pt/dr/lexionario/termo/crime-particular>.

¹⁰⁵ Acórdão TRL de 11-05-2023, proc. n.º 215/20.5T9LSB-C.L1-9, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/650a771605b574f6802589b2004bc175?OpenDocument&Highlight=0,n.º,215%2F20.5T9LSB-C.L1-9>.

A iniciativa parte do MP, na seleção das comunicações com o grande interesse para a descoberta da verdade ou para a prova¹⁰⁶.

Nesse sentido temos esta descrição de como se processam as coisas nesta fase.

Na fase de inquérito, dirigida pelo Ministério Público, é a este que compete decidir o conjunto das diligências que visam a recolha de provas em ordem à decisão sobre a acusação, o que pode/deve ser apreendido e o que tem interesse para a prova.

Em caso de apreensão de mensagens de correio eletrónico, apenas compete ao JIC analisar o que lhe é apresentado, tendo em vista a salvaguarda da reserva da vida privada e de eventuais comunicações entre o arguido e o seu defensor.

A interferência do JIC, limitando o acesso do Ministério Público a mensagens validamente apreendidas viola o princípio do acusatório e a autonomia do Ministério Público, consagrados na Constituição da República Portuguesa¹⁰⁷.

Na fase de instrução, que é dirigida pelo juiz de instrução, será decidido a dedução da pronúncia ou não pronúncia.

Nesta fase decide-se se vai proceder ou não o julgamento, como está previsto no artigo 286.º, n.º 1 do CPP.

Ora, nesta fase, o juiz também pode ordenar, caso necessário, a apreensão das mensagens.

“No que respeita aos procedimentos, no CPP os OPC transmitem a correspondência intacta ao juiz que tiver autorizado ou ordenado a diligência e é este que procede à aberta e primeiro toma conhecimento do seu conteúdo; (...)”¹⁰⁸, depois de tomar o conhecimento do conteúdo das mensagens e considerar relevante para a prova, fá-la juntar ao processo, como é referido na primeira parte do artigo 179.º n.º 3 do CPP.

Ora, a remissão do artigo 17.º da Lei do Cibercrime para o artigo 179.º do CPP, o n.º 3 do último artigo suscita um argumento, ou seja, se há a exigência de ser um juiz a autorizar ou ordenar a diligência e de ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens e só depois juntar ao processo, imaginemos nos casos em

¹⁰⁶ Acórdão TRL de 11-05-2023, proc. n.º 215/20.5T9LSB-C.L1-9 refere que “A intervenção do Juiz de Instrução Criminal em sede de inquérito deve pautar-se por um princípio da intervenção enquanto Juiz das liberdades (e não como Juiz de investigação), respeitando o modelo constitucional de divisão de funções entre a magistratura judicial e a magistratura do Ministério Público.”.

¹⁰⁷ Gabinete Cibercrime (2020) Jurisprudência sobre prova digital, Procuradoria-Geral da República Portuguesa, Nota Prática n.º 16/2020, p. 13.

¹⁰⁸ Cardoso, Rui (2018) - Apreensão de correio electrónico e registo de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX, p. 75, [Consult. 10 dez 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

que existem muitas mensagens para analisar, em termos práticos gera uma grande dificuldade apenas para um juiz, mas tal como a autora Inês Neves refere,

Não há que deixar de exigir que seja o juiz o primeiro a tomar conhecimento do conteúdo do correio electrónico pelas dificuldades práticas de atribuir a um só juiz essa tarefa, mas sim exigir que durante a diligência se tenha sempre em atenção que para a eficácia da mesma devem seguir estritos critérios de abrangência, apenas apreendendo os e-mails que se afiguram realmente determinantes para a prova¹⁰⁹.

No caso de as mensagens não serem relevantes para o grande interesse da descoberta da verdade ou para a prova, o juiz terá de as restituir, não podendo ser utilizadas como meio de prova.

Tudo o que o juiz tomou de conhecimento fica sujeito ao dever de segredo, como é referido na última parte do artigo 179.º, n.º 3 do CPP.

Na Lei do Cibercrime, como a mesma indica no seu artigo 17.º, o juiz tem sempre de dar a autorização ou ordenar a apreensão de correio eletrónico e de registos de natureza semelhante, ou seja, sempre que as autoridades competentes encontrarem este tipo de mensagens que sejam de grande interesse para a descoberta da verdade ou para a prova, terão de pedir autorização ao juiz para procederem à apreensão^{110 111}.

A outra questão a propósito do regime da apreensão do correio eletrónico no artigo 17.º da Lei do Cibercrime é se o juiz tem ou não que ser a primeira pessoa a tomar conhecimento das mensagens de correio eletrónico e registos de comunicação de natureza semelhante.

Há quem defenda, tal como nós, que o juiz não terá de ser necessariamente a primeira pessoa a tomar conhecimentos das mensagens, embora seja quem decide a junção, ou não, das mesmas aos autos como meios de prova¹¹².

Na LCC, durante o inquérito, o Ministério Público, depois de tomar conhecimento do seu conteúdo, deve apresentar ao juiz suporte com as mensagens de correio electrónico ou

¹⁰⁹ Neves, Inês Castanheira, ob. cit., p. 275.

¹¹⁰ Nunes, Duarte Rodrigues, (2021), p. 359.

¹¹¹ Neste sentido, percebe-se a importância e a necessidade de pedir a autorização judicial para se proceder a uma apreensão. Ora, segundo o Acórdão do Tribunal Constitucional n.º 314/2023, que julgou inconstitucional a norma da Lei da Concorrência que permitia à Autoridade da Concorrência proceder ao exame, recolha e apreensão de mensagens de correio eletrónico com mera autorização do Ministério Público, sem despacho judicial prévio.

O Tribunal entendeu que tal regime viola a reserva de juiz e o direito à inviolabilidade da correspondência (arts. 32.º, n.º 4 e 34.º, n.ºs 1 e 4, da CRP). Disponível em <https://www.tribunalconstitucional.pt/tc/acordaos/20230314.html>

¹¹² No mesmo sentido Acórdão Relação de Guimarães de 29-03-2011, proc. n.º 735/10.0GAPTL-A.G1; Nunes, Duarte Rodrigues, (2021), p. 359; contra Acórdão do Tribunal da Relação de Lisboa de 04-02-2020, proc. n.º 1286/14.9IDLBS-A.L1-5; Acórdão do Tribunal da Relação de Lisboa de 10-08-2020, proc. n.º 6330/18.8JFLBS-A.L1-3; Neves, Inês Castanheira, ob. cit., p. 275.

semelhantes cautelarmente apreendidas (ou melhor, os dados informáticos que as constituem), juntamente com o requerimento fundamentado para apreensão daquelas que considere de grande interesse para a descoberta da verdade ou para a prova, após o que o juiz apreciará, tomando conhecimento do seu conteúdo, e decidirá autorizar ou não autorizar a apreensão formal¹¹³.

No mesmo sentido, o autor Pedro Verdelho refere que o regime presente no artigo 179.º do CPP, deve ser aplicado com as devidas adaptações, e a primeira seria a possibilidade de uma apreensão cautelar (que está previsto no artigo 249.º do mesmo diploma) das mensagens de correio eletrónico ou comunicações de natureza semelhante sem a autorização prévia do juiz de instrução¹¹⁴, porque a única exigência legal para a sua apreensão provisória, presente no artigo 17.º da Lei do Cibercrime, é da “(...) existência de uma forma legítima de acesso ao meio informático em que estavam armazenadas.”¹¹⁵.

O mesmo autor, ainda, refere que não se exige que o juiz tenha de ser o primeiro a tomar o conhecimento do conteúdo das mensagens (como acontece com o correio físico), “a letra da lei aponta antes para a possibilidade de quem procede à pesquisa encaminhar para o juiz mensagens concretas, com relevância para o caso concreto, que aquele depois apreenderá ou não.”¹¹⁶.

Ora, quem defende que deve ser o juiz a tomar conhecimento, em primeiro lugar, do conteúdo das mensagens, baseia-se no facto do juiz de instrução ter como função de ser o juiz de direitos, liberdades e garantias e, por isso, ser o único que apresenta competências para autorizar ou ordenar.

Isto é, em caso de apreensão de mensagens, estas estão protegidas pela nossa Constituição (artigo 34.º), mais precisamente, através da proteção ao direito à privacidade e à inviolabilidade da correspondência, devendo, assim, ser o juiz de instrução a tomar conhecimento em primeiro lugar do conteúdo das mensagens como

¹¹³ Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante - artigo 17.º da Lei n.º 109/2009, de 15.IX, p. 75, [Consult. 13 dez 2024].

Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

¹¹⁴ Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX, p. 76, [Consult. 14 dez 2024].

Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

¹¹⁵ Scientia IVRIDICA (2009) Pedro Verdelho - A nova Lei do Cibercrime, Tomo LVIII – N.º 320, p. 743.

¹¹⁶ Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX, p. 77, [Consult. 14 dez 2024].

Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

forma de proteger os direitos fundamentais referidos anteriormente, e garantindo a sua imparcialidade no processo¹¹⁷.

Para sustentar a nossa opinião, podemos ainda abordar o artigo 32.º, n.º 5, da CRP, onde consagra que “O processo criminal tem estrutura acusatória, estando a audiência de julgamento e os actos instrutórios que a lei determinar subordinados ao princípio do contraditório.”

A nossa constituição processual penal tem como um dos princípios estruturantes, o princípio acusatório que, “Essencialmente, ele significa que só se pode ser julgado por um crime precedendo acusação por esse crime por parte de um órgão distinto do julgador, sendo a acusação condição e limite do julgamento.”¹¹⁸, ou seja, na fase de inquérito, deve ser respeitada a função do MP (ação penal) como titular da referida fase do processo e a função do juiz de instrução criminal como juiz de liberdades e garantias¹¹⁹.

Tendo em conta as referidas funções é necessário a separação entre ação e jurisdição, ou seja, o juiz, este deve julgar e não investigar, ao contrário do que acontece com o órgão acusador, que investiga e acusa¹²⁰.

Exposto isto, consideramos que a remissão do artigo 17.º da Lei do Cibercrime para o artigo 179.º, n.º 3, do CPP, onde se estabelece que a tomada de conhecimento, em primeiro lugar, tem de ser realizada pelo juiz de instrução criminal, mesmo na fase de inquérito, e que oficiosamente, ao considerar o conteúdo relevante, fá-lo juntar ao processo, representa uma violação da estrutura acusatória do processo penal, porque tal função (apenas a parte da tomada de conhecimento) compete ao MP como titular na fase de inquérito¹²¹ e como órgão acusador.

¹¹⁷ No mesmo sentido, Acórdão TRL de 07-03-2018, proc. n.º 184/12.5TELSB-B.L1-3, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument> e ainda, Acórdão TRL de 05-05-2022, proc. n.º 305/19.7T9AGH-A.L1-9, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/97c0f4f65870d61e80258847003929a9?OpenDocument>.

¹¹⁸ No mesmo sentido, Gomes Canotilho, José Joaquim e Vital Moreira, (2007), p. 522.

¹¹⁹ No mesmo sentido, Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX, p. 82, [Consult. 16 dez 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

¹²⁰ No mesmo sentido, Acórdão do TC n.º 219/89, proc. n.º 324/88, disponível em <https://www.tribunalconstitucional.pt/tc/acordaos/19890219.html>.

¹²¹ No mesmo sentido, Cardoso, Rui (2018) Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX, p. 85, [Consult. 16 dez 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

Ora, a lei ordinária deve estar conforme a nossa Constituição, sob pena de haver inconstitucionalidade.

3.2 Situações de *periculum in mora*

Após o esclarecimento da competência do JIC e do MP num processo penal e a importância da exigência do pedido de autorização prévia ao juiz de instrução para a devida apreensão do correio eletrónico e de registos de comunicação de natureza semelhante, vamos agora abordar as situações de *periculum in mora*, começando em primeiro lugar, por explicar, de forma breve, no que consiste as medidas cautelares e de polícia.

Vejamos, as medidas cautelares e de polícia, terminologia adotada pelo nosso CPP, estão previstas nos artigos 248.º a 253.º do mesmo diploma, ora, como o seu vocábulo “cautelar” indica, servem para prevenir alguns casos de perigo criminal, neste caso, situações de necessidade e urgência. Ou seja, estas garantem de forma antecipatória a preservação de meios e elementos probatórios¹²².

As medidas cautelares e de polícia são atos que não precisam de autorização prévia da autoridade judiciária, mas terão de ser aplicadas logo após a aquisição da notícia do crime (art. 249.º, n.º 1 do CPP), com o propósito de salvaguardar os meios de prova e/ou outras informações pertinentes para a descoberta da verdade material e que se podiam perder comprometendo assim a investigação criminal¹²³.

Entendemos, que o pressuposto essencial para a aplicação de medidas cautelares e de polícia é a existência de *periculum in mora*¹²⁴.

É importante realçar que estas medidas são da exclusiva competência do OPC¹²⁵, nos termos do artigo 272.º, n.ºs 1 a 3, da CRP, e que apresentam funções de defesa da legalidade e garantem a segurança interna e os direitos dos cidadãos.

¹²² Fernandes Soares, Paulo Alexandre (2017) - Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia, 2ª ed., Almedina Editoras, p. 93.

¹²³ No mesmo sentido, Nunes, Duarte Rodrigues (2023) - Curso de Direito Processual Penal – Tomo II, Elementos do processo penal (continuação). O procedimento criminal. Universidade Católica Editora, p. 221.

¹²⁴ No mesmo sentido, Nunes, Duarte Rodrigues, (2023), p. 221 e Nunes, Duarte Rodrigues, (2021), p. 360.

¹²⁵ Para uma melhor compreensão do conceito é possível consultar a Lei 49/2008, de 27 de agosto (LOIC), mais precisamente, no seu artigo 3.º, n.º 1.

Neste contexto, devido às funções que os OPC apresentam, neste caso, conhecimentos específicos, presença de meios, quer técnicos quer logísticos (art. 2.º, n.º 6 da LOIC), o MP mesmo sendo quem dirige o inquérito, já mais pode dispensar o auxílio dos mesmos durante uma investigação criminal¹²⁶ (art. 263.º, n.º 1 do CPP).

Assim estes tipos de medidas cautelares podem correr mesmo sabendo que os OPC surgem como auxiliares das autoridades judiciárias e atuam no processo de acordo com a sua orientação, havendo uma dependência funcional dos OPC face às autoridades judiciárias (arts. 56.º e 263.º, n.º 2 do CPP)¹²⁷.

Ora, entende-se por dependência funcional “uma delimitação de competências entre as autoridades judiciárias e as polícias, aquelas dirigindo, estas realizando as tarefas de investigação; ...”¹²⁸, havendo assim um clima de cooperação e coordenação durante um processo criminal.

Ainda sobre o artigo 272.º, no seu n.º 2 da CRP, consagra que as medidas de polícia não devem “ser utilizadas para além do estritamente necessário”. Há, assim, que ter em conta o artigo 18.º do mesmo diploma, que consagra o princípio de proporcionalidade (proibição de excesso) onde se destacam os requisitos da necessidade, adequação e proporcionalidade em sentido estrito.

Significa isto, que uma medida de polícia deve consistir numa minimização/ afastamento de um perigo para o interesse público, ou seja, existindo diversas medidas adequadas, a medida escolhida deve ser necessária àquele fim, assim sendo, terá de ser a medida menos gravosa para os direitos fundamentais¹²⁹.

Por fim, a medida sendo adequada e necessária deve ser também proporcional, ou seja, o benefício que ela traz deve ser equivalente ou superior ao sacrifício causado aos direitos fundamentais dos cidadãos¹³⁰.

Como é possível ver, o artigo 55.º, n.º 2, do CPP, consagra que “Compete em especial aos órgãos de polícia criminal, mesmo por iniciativa própria, colher notícia dos crimes e

¹²⁶ No mesmo sentido, Fernandes Soares, Paulo Alexandre, ob. cit., p. 77.

¹²⁷ Acórdão TRL, de 09-06-2016, proc. n.º 50/14.0SLLSB-Y.L1-9, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8cf93372a59dc58480257fd3004a5256?OpenDocument>, e Figueiredo Dias, Jorge de (2024) – Direito Processual Penal. Estudos, 1ª ed., Gestlegal Editora, p. 156

¹²⁸ Figueiredo Dias, Jorge de, ob. cit., p. 158.

¹²⁹ No mesmo sentido, Fernandes Soares, Paulo Alexandre, ob. cit., p. 88 e Canotilho, José Joaquim Gomes e Vital Moreira (2010) – Constituição da República Portuguesa Anotada, Vol. II, 4ª ed., Coimbra Editora, p. 860.

¹³⁰ Idem, *ibidem*.

impedir quanto possível as suas consequências, descobrir os seus agentes e levar a cabo os actos necessários e urgentes destinados a assegurar os meios de prova.”, após colherem a notícia do crime, terão de a transmitir ao MP, num prazo que não pode exceder 10 dias (art. 248.º, n.º 1 do CPP), já nos casos de urgência, a referida transmissão pode ser feita por qualquer meio de comunicação para o efeito disponível, embora a comunicação oral deva ser seguida de comunicação escrita (art. 248.º, n.º 3 do CPP).

Na Lei n.º 109/2009, de 15 de setembro, não existe qualquer capítulo que faça referência às medidas cautelares e de polícia, ao contrário do que se pode ver no CPP, por isso, é necessário analisar se nesta Lei os artigos possibilitam essas medidas.

No seu artigo 11º, na al. c), como já foi referido, consagra a aplicação das disposições processuais, “em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.”

Quanto às medidas cautelares temos desde logo as seguintes normas: o artigo 12.º, n.º 2, que consagra a preservação expedita de dados¹³¹; o artigo 15.º, n.º 3 e 4, que se aplica à pesquisa de dados informáticos¹³²; o artigo 16.º, n.º 2, que refere se à apreensão de dados informáticos¹³³ e, por fim, o artigo 22.º, n.º 4 que trata da preservação e revelação expeditas de dados informáticos em cooperação internacional¹³⁴.

¹³¹ “2- A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.”

¹³² “3- O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

- a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;
- b) Nos casos 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.

4- Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:

- a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;
- b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253º do Código de Processo Penal.”

¹³³ “2- O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.”

¹³⁴ “4- A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior.”

Ora, a pergunta que se suscita é se será possível considerar à luz do artigo 17.º, que corresponde à apreensão do correio eletrónico e registos de comunicação de natureza semelhante, haver apreensão desse correio como medida cautelar e de polícia?

A resposta é sim, pelo simples facto de este artigo remeter para o Código Processo Penal, mais precisamente, para o artigo 179.º referente à apreensão de correspondência que por sua vez, por força do artigo 252.º do CPP que consagra o procedimento de uma medida cautelar e de polícia.

Isto é, em *periculum in mora*, o juiz pode autorizar a abertura imediata da correspondência pelo OPC¹³⁵, e também, o OPC, pode aplicar uma medida cautelar e de polícia segundo o artigo 252.º do CPP, ordenando ao fornecedor de serviço, que suspenda a remessa do correio eletrónico, da SMS, entre outros, devendo ser convalidada por despacho fundamentado pelo juiz, no prazo de quarenta e oito horas, caso contrário, o correio eletrónico e registos de comunicação de natureza semelhante serão remetidos ao respetivo destinatário¹³⁶, tal como é referido no Acórdão do Tribunal da Relação de Lisboa, de 11-01-2011, com o processo n.º 5412/08.9TDLSB-A.L1-5,

Em caso de urgência, isto é, de perda de informações úteis à investigação de um crime em caso de demora, o juiz pode autorizar a abertura imediata de correspondência (assim como de correio electrónico) pelo órgão de polícia criminal e o órgão de polícia criminal pode mesmo ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, nos termos dos n.ºs 2 e 3, do art. 252, do Código de Processo Penal, devendo a ordem policial ser convalidada no prazo de 48 horas, sob pena de devolução ao destinatário caso não seja convalidada, ou caso seja rejeitada a convalidação.¹³⁷

Relativamente, ao Acórdão anterior, não podemos concordar com facto de ser feita a equiparação do correio eletrónico e registos de comunicação de natureza semelhante às encomendas e a valores fechados porque não é essa a natureza daqueles primeiros meios de comunicação, ou seja, não pode ser aplicado o artigo 252.º, n.º 2 do CPP, em situações que estão ao abrigo do artigo 17.º da Lei do Cibercrime¹³⁸.

¹³⁵ Albuquerque, Paulo Pinto de (2023) – Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos, Volume I, 5ª ed., Universidade Católica Editora, p. 792.

¹³⁶ No mesmo sentido, Nunes, Duarte Rodrigues, (2021), p. 360 e Mesquita, Paulo Dá, ob. cit., p. 118.

¹³⁷ Acórdão TRL, de 11-01-2011, proc. n.º 5412/08.9TDLSB-A.L1-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument&Highlight=0,apreensão,correspondência>.

¹³⁸ No mesmo sentido, Nunes, Duarte Rodrigues, (2021), p. 361; contra Acórdão TRL, de 06-02-2018, proc. n.º 1950/17.0T9LSB-A.L1-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument>.

Reforçando a nossa posição, o n.º 2 do referido artigo, consagra uma medida em que o seu objeto material é mais limitado, ao contrário, do que acontece nos n.ºs 1 e 3, porque estes dois últimos, as normas referem-se a qualquer correspondência apreendida ou por apreender, tais como, cartas, encomendas, valores e telegramas, enquanto, o n.º 2 apenas se aplica a encomendas ou valores fechados¹³⁹, como já tinha sido referido atrás.

Exposto isto, entendemos que as medidas cautelares e de polícia no processo penal, especialmente, em situações de perigo de demora, são importantes para a preservação dos meios de prova que podem ser fundamentais para a investigação criminal. E nesses casos os OPC, ao aplicarem uma medida cautelar e de polícia, de acordo com o artigo 252.º do CPP, essa medida terá de ser convalidada por despacho fundamentado ao juiz no prazo de quarenta e oito horas.

Assim a apreensão prevista no artigo 17.º da Lei do Cibercrime pode surgir como uma medida cautelar e de polícia, por causa da remissão para o artigo 179.º do CPP. Ao fazer essa remissão está-se, por sua vez, a remeter para o artigo 252.º do mesmo diploma e a permitir a prática de medidas cautelares e de polícia.

Há, no entanto, que ter em conta que face à natureza do correio eletrónico não se aplica o n.º 2 deste último artigo.

Seguiremos para a explicação do processo de valoração das provas obtidas nos casos de perigo na demora.

3.2.1 Posterior valoração das provas obtidas neste modo

Como se pode retirar do dito atrás, muitas das vezes, os grandes sucessos das investigações criminais estão dependentes do trabalho efetuado pelos OPC, que garantem a proteção de provas relevantes para o grande interesse da descoberta da verdade material. Tal implica que os OPC, “mesmo antes de receberem ordem da autoridade judiciária competente para procederem a investigações, possam praticar os

¹³⁹ No mesmo sentido, Albuquerque, Paulo Pinto de (2023) - Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos, Volume II, 5ª ed., Universidade Católica Editora, p. 67.

actos cautelares necessários e urgentes para assegurar os meios de prova.” (art. 249.º, n.º1 do CPP).

Esta forma de adquirir provas sem previa autorização da autoridade judiciária, tal como já referido em cima, terá de ser realizada de acordo com o que está previsto na lei para não existir a violação dos direitos fundamentais dos cidadãos, caso contrário, torna-se proibida a utilização desses meios de prova no processo¹⁴⁰.

Uma das normas a que essas medidas têm de obedecer está no artigo 253.º do CPP, de acordo com o qual um relatório deve ser remetido à autoridade judiciária competente, independentemente da fase do processo, e só nesse caso se garante a admissibilidade da prova e o respeito pelos direitos fundamentais.

Tendo em conta o artigo 253.º do CPP, o relatório trata-se de um instrumento em que a autoridade judiciária controla a atividade cautelar do OPC¹⁴¹, pelo que o mesmo deve ser dirigido à autoridade judiciária competente para a sua validação, no entanto, o relatório deve ser “(...) minucioso, descrevendo as investigações feitas e os resultados das mesmas, isto é, os meios de prova e de obtenção de prova recolhida e os factos apurados (...)”¹⁴².

No n.º 2 do mesmo artigo, é permitido que o relatório seja enviado ao MP ou ao Juiz de Instrução, dependendo da titularidade da fase processual e em função da competência material de cada autoridade judiciária. A título de exemplo se o caso se tratar da suspensão da remessa da correspondência (art. 252.º, n.º 3 do CPP) esta matéria será da competência do JIC, por isso, o relatório deve ser dirigido a este, independentemente, destes atos cautelares ocorrerem em fase pré-processual, ou durante o inquérito ou, ainda, em fase de instrução¹⁴³.

4. Grau de suspeita exigido para o procedimento do respetivo artigo

O artigo 17.º da Lei do Cibercrime, como já referido várias vezes, remete para o artigo 179.º do CPP que prevê o regime da correspondência. Ora, este último artigo, tal como

¹⁴⁰ No mesmo sentido, Nunes, Duarte Rodrigues (2021), p. 361 e também, Fernandes Soares, Paulo Alexandre, ob. cit., p. 132.

¹⁴¹ Albuquerque, Paulo Pinto, (2023b), p. 72.

¹⁴² Idem, *ibidem*.

¹⁴³ Idem, pp. 72 e 45.

o artigo 17.º não fazem qualquer referência ou até mesmo uma exigência em matéria de grau de suspeita exigido para utilizar este meio de obtenção de prova.

No entanto, existe a proibição do excesso e por isso quando os dados que irão ser obtidos contenham informações que possam ser integradas na esfera íntima, à luz da nossa Constituição, se deve exigir uma suspeita fundada¹⁴⁴.

Dito de outra forma, durante a investigação a obtenção destes dados pode afetar os direitos fundamentais dos cidadãos, como a privacidade, e por isso, a intervenção deverá ser rigorosa e, principalmente, proporcional.

Exposto isto, só é exigido o grau de suspeita no artigo 17.º da Lei n.º 109/2009, quando os dados envolvam a esfera íntima.

No caso de haver uma denúncia anónima, esta pode desencadear a abertura do inquérito como também irá permitir o recurso à apreensão de correio eletrónico e de registos de comunicação de natureza semelhante¹⁴⁵.

Neste caso para se proceder à apreensão de correio eletrónico e de registos de comunicações de natureza semelhante, a denúncia tem de estar ao abrigo do artigo 246.º, n.º 6 do CPP. Assim, só será possível a abertura de um inquérito se dela resultarem indícios da prática de um crime ou, ainda, constituir um crime tipificado por lei, neste caso, será o MP, no exercício da ação penal, a decidir a relevância jurídica da denúncia anónima ou a sua destruição^{146 147}.

Quando o processo já se encontra em fase de inquérito, a que foi dirigida a denúncia anónima, compete ao MP decidir sobre os eventuais factos relatados ou a destruição da mesma¹⁴⁸.

No caso de o processo estar na fase de instrução, julgamento ou recurso e ser dirigida uma denúncia anónima o juiz em questão (de instrução, presidente ou relator) deve mandar para o MP para este se pronunciar sobre a relevância da dita denúncia, no

¹⁴⁴ No mesmo sentido, Nunes, Duarte Rodrigues (2019) – O problema da admissibilidade dos métodos “ocultos” de investigação criminal como instrumento de resposta à criminalidade organizada, 1ª ed., Gestlegal Editora, p. 628.

¹⁴⁵ No mesmo sentido, Nunes, Duarte Rodrigues, (2021), p. 354.

¹⁴⁶ Caso seja ordenado a destruição da denúncia anónima, esta deve ser registada num auto, com a indicação da hora e da data da diligência, da autoridade que ordenou o ato e do funcionário que o realiza, do número de entrada da denúncia no registo de denúncias e do meio utilizado para a sua destruição.

¹⁴⁷ Albuquerque, Paulo Pinto de, (2023 b), p. 36.

¹⁴⁸ Idem, p. 36.

entanto, se o MP considerar que não revela indícios da prática de um crime nem constitui um crime (art. 246.º, n.º 6 do CPP), o juiz depois irá ordenar a sua destruição¹⁴⁹.

¹⁴⁹ Idem, *ibidem*.

Capítulo 4: Enquadramento jurídico-constitucional deste meio de prova

1. Direito fundamental à reserva da vida privada

A apreensão do correio eletrónico e de registos de comunicação de natureza semelhante consiste no acesso ao conteúdo das mensagens armazenadas no sistema informático que sejam importantes para a descoberta da verdade material e para a prova.

O direito à reserva da intimidade da vida privada, que está previsto no artigo 26.º, n.º 1, 32.º, n.º 8, 35.º e 268.º, n.º 2 da CRP¹⁵⁰, pode ser afetado com esta prova.

Já o direito à inviolabilidade das comunicações (art. 34.º, n.º 4 do mesmo diploma), a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante para a maior parte da doutrina não o restringe porque o ato comunicacional, em sentido estrito, já cessou e, por este motivo, já não apresenta uma situação de perigo ou carência da proteção constitucional da inviolabilidade das comunicações¹⁵¹.

Assim, o artigo 17.º da Lei do Cibercrime, restringe apenas os direitos à intimidade/privacidade, à palavra virtual, e à autodeterminação informacional.

Estaremos sempre perante uma ofensa a direitos fundamentais, principalmente do direito à reserva da vida privada¹⁵², que merecem uma tutela adequada e proporcional, tema que será desenvolvido mais à frente.

Isto é, as normas do CPP devem estar em sintonia com as normas e princípios da nossa Constituição de forma a garantir o equilíbrio entre os direitos, liberdades e garantias protegidos constitucionalmente e os objetivos que o processo penal apresenta.

Importa ainda referir, que quando se procede a uma apreensão de mensagens, enquanto meio de prova que interfere com os direitos ligados à esfera privada, pode

¹⁵⁰ Bem como nos artigos 12.º da DUDH; artigo 8.º da CEDH; artigos 7.º e 8.º da CDFUE.

¹⁵¹ Nunes, Duarte Rodrigues (2021), pp. 349 e 350; contra, Acórdão TRL de 11-07-2019, proc. n.º 184/12.5TELSB-B.L1-3, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1bc410315a7483298025843b004c1e71?OpenDocument>.

¹⁵² Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX p. 66, [Consult. 26 fev. 2025]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>.

afetar mais do que uma pessoa, ou seja, tanto o remetente da mensagem como o destinatário que a irá receber¹⁵³. Esta situação pode gerar alguns problemas de identificação do titular do bem jurídico afetado.

2. Proteção da palavra escrita e da palavra falada

Com a evolução do ser humano, permitiu que ao longo dos anos fosse possível assistir à evolução da comunicação, sendo ela a comunicação oral, gestual e, por fim, a escrita.

Essa comunicação implica a emissão e exteriorização de uma mensagem e consequentemente a comunicação entre duas ou mais pessoas¹⁵⁴.

A comunicação oral é considerada a expressão superior de uma relação comunicacional pois a transmissão da comunicação dá-se num curto espaço de tempo e com uma quantidade certa e precisa de fluxo informacional. Já a palavra escrita (posteriormente a palavra virtual) veio permitir o mesmo fluxo informacional em qualquer suporte físico e/ou digital e para todas as partes do mundo¹⁵⁵.

Como referimos anteriormente, através do correio eletrónico a mensagem poder ser transmitida na forma de texto, de voz, de som ou imagem, e por isso, podem pôr em causa diferentes questões quanto à proteção constitucional.

Vejamos, a palavra falada (em tempo real), está presente no artigo 26.º, n.º 1 da CRP, enquanto, que a palavra escrita não é referida neste artigo pelo simples facto de a primeira requerer uma maior proteção, pois existem três direitos que devem ser tidos em conta, neste caso,

- (a) *Direito à voz*, como atributo de personalidade, sendo ilícito, sem consentimento da pessoa, registar e divulgar a sua voz (com ressalva, é claro, do lugar em que ela foi utilizada);
- (b) *direito às «palavras ditas»*, que pretende garantir a autenticidade e o rigor da reprodução dos termos, expressões, metáforas escritas e ditas por uma pessoa;
- (c) *direito ao auditório*, ou seja, a decidir o círculo de pessoas a quem é transmitida a palavra¹⁵⁶.

¹⁵³ Acórdão TRL de 24-09-2013, proc. n.º 145/10.9GEALM.L2-5. Disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c60dfe830c97cf8980257c0000368afa?OpenDocument>.

¹⁵⁴ Freitas, José Pedro, ob. cit., p. 92.

¹⁵⁵ Idem, *ibidem*.

¹⁵⁶ Canotilho, José Joaquim e Vital Moreira (2007), p. 467.

Já a palavra escrita, quando enviada, fica perpetuada no mundo virtual, por isso, a comunicação privada escrita poderá pôr em causa não só a inviolabilidade das comunicações, como da privacidade, mas já não o direito à palavra falada¹⁵⁷.

A palavra já não pertence a ninguém.

É, em exaltação do fragmentário, pedaço para todos.

Pode ser apagada, riscada com a brevidade do gesto da negação.

Pode ser criada, recriada, transformada ou desencantada com a subtileza ou a persistência dos conquistadores do nada ou no tempo de um olhar.

Mas pode, para além de tudo, ser fonte de informação, lugar de procura do conhecimento, átrio da perplexidade do pensar e sempre ponto de encontro do modo-de-ser humano¹⁵⁸.

Apesar da palavra escrita não ter a mesma proteção que a palavra falada, tal não significa que a primeira depois de enviada, após o processo de comunicação ter terminado, perca a sua proteção constitucional, a proteção apenas fica ao abrigo do artigo 35.º da CRP. Isto é, a sua proteção se rege na privacidade na utilização da informática, ou seja, o direito à autodeterminação informacional, consiste em proteger o cidadão nos momentos de recolha, armazenamento, utilização e transmissão dos seus dados pessoais¹⁵⁹.

A este propósito da proteção da palavra falada e escrita importa referir que José De Faria Costa considera que a nossa tecnologia criou outra palavra, a palavra virtual,

a informática, mas sobretudo a informatização em rede, veio trazer a possibilidade de a palavra não ser escrita, nem falada, estar virtualmente visível em um écran por força de um jogo complexo cingido à simples lógica binária.

O que permite a possibilidade de a palavra estar e não estar e, todavia, se se quiser, estando ou não estando, trazê-la ao mundo normal da palavra escrita em suporte de papel¹⁶⁰.

Ainda quanto a este tema da palavra importa ressaltar que temos situações como, por exemplo, na aplicação do WhatsApp, em que é possível utilizar a palavra escrita, como a palavra falada, neste caso.

Assim, se existir uma comunicação em videochamada a palavra deve ser protegida ao abrigo do artigo 26.º da nossa Constituição, porque a comunicação ocorre em tempo real.

¹⁵⁷ Neves, Rita Castanheira, ob. cit., pp. 46 e 47.

¹⁵⁸ Costa, José Faria (1998) - Direito Penal da Comunicação (Alguns escritos), Coimbra Editora, p. 152.

¹⁵⁹ Idem, p. 58.

¹⁶⁰ Idem, p. 49, *apud* Costa, José De Faria, "As telecomunicações e a privacidade...", pp. 151 e 152.

Neste âmbito surge outra questão fundamental: as mensagens de voz devem ser equiparadas ou até mesmo apresentarem a mesma proteção constitucional da palavra falada em tempo real?

Creemos que não, porque a transmissão da mensagem de voz consiste numa gravação e depois é enviada para o respetivo destinatário, por isso, consideramos que a proteção que lhe deve ser atribuída é a da palavra escrita.

O facto de a palavra falada em tempo real estar relacionada com o regime das escutas telefónicas o mesmo não acontece com as mensagens de voz, porque as primeiras são proferidas no momento, ou seja, “(...) numa conversação telefónica projecta a mais instantânea realização da personalidade do Homem posta num acto comunicacional, exigindo por isso uma protecção acrescida, (...)”¹⁶¹, enquanto que, as segundas são classificadas como um grau de ponderação igual à palavra escrita, pois irá continuar “(...) para além do acto em que chega ao destinatário da comunicação.”¹⁶², neste caso, pode ser eliminada ou então ser ouvida mais do que uma vez, porque fica armazenada no sistema informático.

Exposto isto, o correio eletrónico pode ser enviado em forma de mensagem escrita, sonora ou ainda uma imagem, o que revela que é utilizado a palavra escrita e a palavra falada, sendo que esta última é gravada, não tendo a mesma proteção constitucional da palavra falada em tempo real, como acontece nas videochamadas, numa comunicação telefónica, numa conversa entre duas pessoas, pessoalmente, ou até mesmo num auditório.

Assim, entendemos que a mensagem de voz, transmitida via correio eletrónico, mas não só, jamais pode ser equiparada ou até mesmo apresentar a mesma proteção da palavra falada em tempo real que está protegida constitucionalmente pelo artigo 26.º (CRP), pelo simples facto de poder ser ouvida mais que uma vez ou ser eliminada.

3. Princípio da proporcionalidade

Tendo em conta o que foi dito anteriormente, sempre que se proceder a uma apreensão de correio eletrónico e de registos de comunicação de natureza semelhante existe

¹⁶¹ Neves, Rita Castanheira, ob. cit., p.179.

¹⁶² Idem, *ibidem*.

restrição de direitos fundamentais, por isso, terá de se ter em conta os ditames do princípio da proporcionalidade.

A referida apreensão deverá ser adequada para que a obtenção de dados informáticos possa servir de prova durante o processo (adequação)¹⁶³; a mesma deverá ser igualmente necessária no sentido de ser a menos onerosa para a pessoa afetada, tal implica que se outros meios de obtenção de prova menos onerosos permitiriam alcançar o mesmo objetivo pretendido com a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante serão esses que devem ser utilizados (necessidade)¹⁶⁴; e por fim, os direitos fundamentais do visado não podem sofrer um sacrifício excessivo face à gravidade do crime que se encontra em investigação e à importância das provas dos dados informáticos em causa, porém, é necessário realizar uma ponderação constitucionalmente adequada entre os interesses em conflito¹⁶⁵, ou seja, “os meios legais restritivos e os fins obtidos devem situar-se numa «justa medida», impedindo-se a adopção de medidas legais restritivas desproporcionadas, excessivas, em relação aos fins obtidos.” (proporcionalidade *stricto sensu*)¹⁶⁶.

Exposto isto, o princípio da proporcionalidade é muito importante para que não exista decisões injustas e que, principalmente, se violem os direitos, liberdades e garantias dos cidadãos que estão protegidos pela nossa Constituição e também os direitos consagrados na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia dos Direitos do Homem, que vamos abordar no subtítulo seguinte.

4. Proteção de dados pessoais (CDFUE) e Privacidade (CEDH)

Porque por vezes o correio eletrónico inclui dados pessoais importa tratar da sua proteção aqui.

¹⁶³ Nunes, Duarte Rodrigues, (2021), p. 350.

¹⁶⁴ Idem, *ibidem*.

¹⁶⁵ Idem, pp. 350 e 351.

¹⁶⁶ Canotilho, José Joaquim e Vital Moreira, (2007), p. 393.

Os dados das pessoas singulares é um direito fundamental protegido pela Carta dos Direitos Fundamentais da União Europeia (CDFUE), previsto nos artigos 7.^o¹⁶⁷ e 8.^o¹⁶⁸, tal como, na nossa Constituição.

No primeiro diploma é defendido que todos nós temos direito à proteção dos nossos dados pessoais e que só podem ser acedidas de acordo com o nosso consentimento¹⁶⁹, porém, nas situações em que está a decorrer uma investigação criminal, as entidades competentes podem aceder aos nossos dados pessoais sem a nossa autorização.

No entanto, para que não haja violação dos nossos direitos, o acesso tem de ser realizado pelas entidades competentes, tendo em conta os procedimentos e requisitos fundamentais, anteriormente, abordados.

Só assim se procederá de forma justa e legal a uma apreensão de correio eletrónico e de registos de comunicação de natureza semelhante.

O direito à proteção dos dados pessoais, não se trata assim de um direito absoluto e tal como o Acórdão do Tribunal da Relação de Lisboa afirma, este direito deve “(...) ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.”¹⁷⁰.

¹⁶⁷ Artigo 7.º do CDFUE: “Todas as pessoas têm direito ao respeito pela vida privada e familiar, pelo seu domicílio e pelas suas comunicações.”. EUR-Lex – Access to European Union law, CDFUE. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12016P%2FTXT>.

¹⁶⁸ Artigo 8.º do CDFUE:

“1- Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
2- Esses dados devem ser objecto de um tratamento leal, para fins específicos e com consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei.
Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.

3- O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”. EUR-Lex – Access to European Union law, CDFUE. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12016P%2FTXT>.

¹⁶⁹ No mesmo sentido, Acórdão TJUE, de 07-03-2024, proc. n.º C-604/22, disponível em <https://curia.europa.eu/juris/document/document.jsf?text=&docid=283529&pageIndex=0&doclang=PT&moe=req&dir=&occ=first&part=1&cid=1203>.

¹⁷⁰ Acórdão TRL, de 02-05-2023, proc. n.º 12234/21.0T8LSB.L1-7, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6b57c49941d5779f802589aa0049be2a?OpenDocument>.

Relativamente, ao artigo 8.º da CEDH¹⁷¹, este é considerado, segundo o Acórdão Satakunnam Markkinapörssi oy e Satamedia oy c. Finlândia¹⁷², como “uma dimensão de autodeterminação informacional”, em que permite aos cidadãos terem o direito à privacidade, ou seja, os elementos recolhidos, tratados e divulgados após um processamento conjunto, ficarão ao abrigo do referido artigo¹⁷³.

Na nossa doutrina, o direito à autodeterminação informacional está presente no artigo 35.º da CRP, em que é protegida a informação disponível sobre os dados pessoais de um cidadão, pois, este consegue assegurá-la de forma que não seja possível recolhê-la, armazená-la, utilizá-la e transmiti-la sem restrições¹⁷⁴.

No entanto, segundo os n.ºs 2 e 4, in fine do mesmo artigo, este direito não é absoluto, sendo, por vezes, sujeito a algumas restrições para que haja a proteção de outros direitos fundamentais¹⁷⁵, sendo necessária uma autorização prévia emitida pela Comissão Nacional da Proteção de Dados (CNPd).

A CNPD, consiste numa entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, o que permite controlar e fiscalizar o cumprimento da RGPD, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, assegurando assim, a defesa dos direitos, liberdades e garantias das pessoas singulares¹⁷⁶.

Para uma melhor compreensão deste artigo, vamos analisar um Acórdão do Tribunal Europeu dos Direitos Humanos (TEDH).

O caso que vamos abordar é do Acórdão do Tribunal dos Direitos Humanos, Laurent C. França, de 24-05-2018¹⁷⁷, em que um oficial de polícia pediu a cada um dos arguidos

¹⁷¹ Artigo 8.º da CEDH: “1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2- Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.”.

Convenção Europeia dos Direitos do Homem. Disponível em https://www.echr.coe.int/documents/d/echr/convention_por.

¹⁷² Albuquerque, Paulo Pinto de (org.) (2019) – Comentário da Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais, Volume II, Universidade Católica Editora, p. 1439.

¹⁷³ Idem, *ibidem*.

¹⁷⁴ No mesmo sentido, Nunes, Duarte Rodrigues, (2019), p. 237.

¹⁷⁵ Idem, p. 239.

¹⁷⁶ Comissão Nacional de Proteção de dados (CNPd). Disponível para consulta em <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>.

¹⁷⁷ Acórdão TEDH Laurent C. França – 28798/13, de 24-05-2018, disponível em [https://hudoc.echr.coe.int/fre - {\"itemid\":\"001-183129\"}\]](https://hudoc.echr.coe.int/fre - {\).

para ver as folhas que o advogado deu a pedido dos mesmos, com os seus dados de contacto escrito à mão para posteriormente poderem comunicar com o ele relativamente à sua defesa.

A pedido do oficial de polícia, os arguidos deram as folhas e de seguida o mesmo devolveu-as.

O advogado Laurent após algumas tentativas, queixou se finalmente ao TEDH por violação do artigo 8.º da CEDH, direito à vida privada e familiar, na vertente do direito ao respeito da confidencialidade da correspondência entre um advogado e os seus constituintes.

O Tribunal admitiu a queixa, tendo o Conselho Nacional da Ordem dos Advogados intervindo na qualidade de terceiro interveniente em que defende a proteção da confidencialidade das comunicações entre o advogado e o seu constituinte.

No decorrer do processo, levantou se a questão de saber se a entrega de uma folha dobrada com dados de contacto do advogado se insere na noção de correspondência.

O Tribunal considerou que sim, e entendeu que existia um fundamento válido de interceção da correspondência, justificando por razões de segurança e para prevenir o cometimento eventual de uma infração pelos arguidos, ou seja, tendo em conta o teste de proporcionalidade, o mesmo explicou que a relação entre o fim legítimo da medida e a sua necessidade numa sociedade democrática, pode haver um controlo de correspondência de uma pessoa detida, mas entre um advogado e os seus constituintes existe um estatuto privilegiado pela função específica do advogado na realização da justiça.

Relativamente, à posição do oficial de polícia, este agiu de forma a prevenir um ato perigoso, mas nunca fundamentou a sua conduta, nem justificou de alguma forma que este papel pudesse ter conteúdo perigoso.

Por isso, a interceção de correspondência realizada não foi legítima, e o MP ainda referiu que a dita interceção foi ofensiva em relação ao princípio da livre comunicação entre o advogado e os seus constituintes.

Exposto isto, concluiu se que foi ilegítimo e existiu de facto uma violação do artigo 8.º da CEDH, no entanto, ficamos a perceber a diferença entre ambos os artigos (art. 8.º da CDFUE e o art. 8.º da CEDH), ora o primeiro artigo aborda de forma mais específica a proteção dos dados pessoais dentro da União Europeia, enquanto o segundo artigo

prevê o tema da privacidade de forma mais ampla, ou seja, na proteção da vida privada, neste caso, da correspondência.

Porém, ambos garantem uma proteção contra as violações realizadas durante as investigações criminais, quando procedem às apreensões de correio eletrónico e de registos de comunicação de natureza semelhante.

Capítulo 5: Tratamento jurisprudencial deste meio de obtenção de prova

1. Divergência no tratamento a dar ao correio aberto e fechado

Terminada a análise do enquadramento jurídico-constitucional da apreensão do correio eletrónico e registo de comunicação de natureza semelhante, chegámos ao último ponto deste trabalho, que suscita mais dúvidas: quando o remetente envia uma mensagem ou um email para um destinatário, este último irá decidir se a vai ler ou não, seja qual for a sua decisão, esta mensagem fica armazenada no seu respetivo dispositivo.

A questão é se poderá existir a apreensão dessa mensagem quando o destinatário não tenha lido tal comunicação?

Apesar deste capítulo ser direcionado para a posição jurisprudencial importa começar por expor a doutrina antes da entrada em vigor da Lei do Cibercrime e do seu artigo 17.º, mas após a reforma do CPP em 2007 e o seu artigo 189.º.

O autor Pedro Verdelho, a propósito do correio eletrónico, defende que o regime a aplicar varia consoante o momento da apreensão. O mesmo sugere a aplicação de um regime tripartido no que respeita à obtenção de prova digital, distinguindo da seguinte forma:

- 1) se tivermos perante um caso de interceção em tempo real de uma comunicação eletrónica devemos aplicar o regime das interceções telefónicas, nos termos do artigo 189º do CPP;
- 2) se a comunicação eletrónica chegou ao seu destino, mas ainda não foi lida, então a comunicação cessou e encontra-se no dispositivo tecnológico do destinatário à espera de ser lida, como tal será um ficheiro em formato digital e deverá ser aplicado o regime da apreensão de correspondência, previsto no artigo 179º do CPP;
- 3) Se a comunicação eletrónica já foi recebida, aberta e lida, então o meio de obtenção de prova que deverá ser aplicado será o das normais apreensões, previsto no artigo 178 do CPP.¹⁷⁸.

Nesta situação estamos perante três momentos distintos, e tal como o autor indica “[...] então teremos obrigatoriamente de ter três regimes completamente distintos.”¹⁷⁹.

¹⁷⁸ Freitas, José Pedro, ob. cit., pp. 134 e 135, *apud* Verdelho, Pedro (2005) - A obtenção de prova no ambiente digital, pp. 121-124.

¹⁷⁹ Idem, p.135.

Ora, na primeira situação o autor defende que se uma comunicação eletrónica está a ser enviada deverá ser aplicado o regime das interceções telefónicas, já na segunda situação, onde a mensagem já foi enviada mas não lida o regime será a apreensão de correspondência (artigo 179.º do CPP), pois essa mensagem ficará armazenada no dispositivo do destinatário ou no servidor, por fim, a terceira situação em que o destinatário recebeu e leu a mensagem, esta perde a definição de comunicação em transmissão e passa a ter a mesma essência de uma correspondência em papel, ou seja, é considerada como um mero documento escrito, que pode ser apreendido durante uma busca^{180, 181}.

Porém, segundo o autor Benjamim Silva Rodrigues, que tem uma visão tripartida semelhante, defende que a monitorização de comunicações eletrónicas, em tempo real, terá neste caso, de ser aplicado o regime previsto no artigo 189.º do CPP¹⁸², na segunda situação, em que a comunicação se encontra na posse do destinatário, mas que ainda não foi aberta nem lida, o mesmo defende que, “[...] se trata de uma comunicação em trânsito, tendo em conta que está dependente de recolha, como tal, também aqui a obtenção de prova digital deve ser regida de acordo com o regime das escutas telefónicas.”¹⁸³.

Quando a comunicação foi recebida, aberta e lida, este autor vem defender que estamos perante um documento “detentor de dados pessoais” e não de um documento eletrónico, ficando assim ao abrigo nos termos da Lei n.º 41/2004, de 18 de agosto (Proteção de Dados Pessoais e Privacidade nas Telecomunicações) e da Lei n.º 67/98, de 26 de outubro¹⁸⁴ (Lei da Proteção de Dados)¹⁸⁵.

Já a teoria defendida por Manuel da Costa Andrade, é que a comunicação só existe até a mensagem ficar na posse do destinatário, ou seja, o mesmo refere que é “[...]”

¹⁸⁰ Idem, *ibidem*.

¹⁸¹ Temos como exemplo o Acórdão do Tribunal da Relação de Lisboa de 15-07-2008, com o proc. n.º 3453/2008-5, que refere: “As mensagens que, depois de recebidas, ficam gravadas no receptor deixam de ter a natureza de comunicação em transmissão, nesta perspetiva, são comunicações recebidas, pelo que deverão ter o mesmo tratamento da correspondência escrita já recebida e guardada pelo destinatário tal como acontece na correspondência efetuada pelo correio tradicional, diferenciar-se-á a mensagem já recebida mas ainda não aberta da mensagem já recebida e aberta.”

Disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/9182245992c7c5d18025749000503b8c?OpenDocument&Highlight=0.SMS>. [Consult. 18 nov. 2024].

¹⁸² Freitas, José Pedro, ob. cit., p.139 *apud* Rodrigues, Benjamim Silva (2008) Das escutas telefónicas - Tomo I, A monitorização dos fluxos informacionais e comunicacionais, Coimbra Editora, pp. 442-450.

¹⁸³ Freitas, José Pedro, ob. cit., p. 139.

¹⁸⁴ O Diploma referido foi revogado pela Lei n.º 58/2019, de 8 de agosto.

¹⁸⁵ Freitas, José Pedro, ob. cit., p. 139.

incompreensível a redação dada pelo legislador português ao art.º 189.º do CPP.”¹⁸⁶, porque durante este processo de transmissão existe a proteção das comunicações eletrónicas, mas acaba quando o destinatário recebe e lê a mensagem.

Exposto isto, percebemos que este autor defende que após a mensagem ter sido recebida, lida e guardada no dispositivo do destinatário, esta comunicação passa a valer como um mero documento escrito sendo objeto de busca (apreensão do computador ou telemóvel), porque

(...) passa a dispor de meios de autotutela, desde a instalação de sistemas de segurança, programas anti-vírus, codificação criptica, firewalls (programas que vigiam o tráfego na internet e avisam o titular do computador das tentativas de envio de programas do género “cavalo de Tróia”), até ao apagamento ou destruição, pura e simples dos dados¹⁸⁷.

Com uma teoria totalmente oposta, temos a do autor Rogério Bravo, que enumerou um conjunto de argumentos que o levam a não considerar a equiparação do correio eletrónico armazenado no sistema informático à correspondência fechada, pois o mesmo afirmou que as mensagens de correio eletrónico quando são recebidas num sistema informático passam a ser meros dados informáticos armazenados localmente, como se fossem uma folha de cálculo, e, por este motivo, estas mensagens já mais poderão ser equiparadas ao conceito tradicional de correspondência por carta¹⁸⁸.

Como primeiro argumento, o autor referiu que na pesquisa do conceito de correspondência em outras legislações, não é provável alcançar apoio na aplicação do regime de correspondência ao regime das comunicações eletrónicas, no entanto, ainda propõem o artigo 194.º do CP, não faz referência às comunicações eletrónicas digitais, porque só se refere a expressões como “carta”, “encomendas”, e “escrito fechado”, que têm como significado de correspondência corpórea¹⁸⁹.

O autor ainda defende que nenhum dos direitos, liberdades e garantias de um cidadão devem ficar dependentes da tecnologia, pelo facto de

o utilizador médio das novas tecnologias cai muitas vezes na tentação de equiparar a correspondência tradicional ao correio-electrónico, principalmente quando o faz a partir da conjugação da percepção de que ele é o destinatário de uma mensagem que lhe é enviada por um remetente, mensagem essa marcada “à chegada” ao seu sistema informático pela sinalética habitual constante dos programas clientes de correio-

¹⁸⁶ Freitas, José Pedro, ob. cit., p. 140 *apud* Andrade, Manuel da Costa (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, pp. 158-159.

¹⁸⁷ Freitas, José Pedro, ob. cit., p. 141 *apud* Andrade, Manuel da Costa, ob. cit., p. 160.

¹⁸⁸ Bravo, Rogério, ob. cit., p. 3.

¹⁸⁹ Bravo, Rogério, ob. cit., p. 4.

electrónico, que é a regra exhibe uma imagem de um envelope de correio fechado, imagem essa que desaparece (ou se transforma) assim que é voluntariamente “aberta” (acedida, mas não necessariamente lida)¹⁹⁰.

Como sabemos, grande parte dos programas dá a possibilidade ao utilizador de remarcar sem limite de vezes as mensagens lidas, como não lidas¹⁹¹.

Exposto isto, o autor adota uma posição bipartida. Num primeiro momento, enquanto a mensagem se encontra em trânsito, deve ser aplicado o regime das escutas telefónicas, garantindo se assim a proteção da própria comunicação.

Num segundo momento, após a mensagem ter chegado ao destinatário, esta deixa de beneficiar dessa tutela e passa a ser equiparada a um simples documento escrito, não precisando de qualquer proteção adicional.

A autora Rita Castanheira Neves, também defende uma visão bipartida do regime de obtenção de comunicações eletrónicas.

A autora começa por não concordar com o alargamento imoderado do regime das escutas telefónicas previsto no artigo 189.º do CPP, porque este alargamento a outro tipo de comunicações não pode ser a solução, pelo simples facto da violação dos direitos pessoais variar consoante os diferentes tipos de comunicações.

Além disso, devem ter diferentes graus de intensidade e não por se tratar de um telemóvel, telefone ou a internet, ou seja, a diferenciação entre os regimes deve se basear pela própria comunicação, mais precisamente, pela distinção da palavra falada e da palavra escrita¹⁹², por isso, a autora defende que o regime das escutas telefónicas deve corresponder apenas à comunicação oral¹⁹³.

Exposto isto, a autora defende que entre o primeiro momento em que a comunicação é enviada até que essa mensagem seja aberta e eventualmente lida, terá de ser aplicado um regime autónomo das interceções de comunicações eletrónicas para se recolher o conteúdo da mensagem num processo de investigação¹⁹⁴.

Obviamente que a mensagem não perde o seu interesse para a investigação criminal por já não ser comunicação trânsito.

¹⁹⁰ Idem, pp. 6 e 7.

¹⁹¹ Idem, *ibidem*.

¹⁹² A autora refere que “a primeira extingue-se no momento em que é proferida, não sendo suposto haver qualquer perpetuação, a segunda já terá um carácter imortalizado” – Freitas, José Pedro, ob. cit., p. 144 *apud* Neves, Rita Castanheira, ob. cit.

¹⁹³ Freitas, José Pedro, ob. cit., pp. 143 e 144 *apud* Neves, Rita Castanheira, ob. cit., p. 176.

¹⁹⁴ Freitas, José Pedro, ob. cit., p. 144.

Aliás, mantém o teor da mensagem o mesmo interesse investigatório que tinha antes de iniciar o seu percurso comunicacional.

O que se altera é o seu estatuto, o que muda é o seu estado¹⁹⁵.

No segundo momento, quando a mensagem é aberta e lida, a autora defende que a mesma passa a ser um ficheiro em formato digital que pode ser buscado/ apreendido e se

houver interesse e legitimidade para os mesmo constarem dos autos, o meio através do qual se efectuará a obtenção de prova é o registo ou cópia dos suportes digitais, sendo certo, pois, que a apreensão propriamente dita será já relativa aos suportes/ objectos físicos que contêm os conteúdos gravados¹⁹⁶.

Como última opinião doutrinária, destaca-se a posição do autor Armando Dias Ramos, que defende que o segredo das comunicações eletrónicas terá proteção enquanto a mensagem se encontrar em trânsito, depois de chegar ao dispositivo do destinatário, ou seja, quando este a receber, perde a tal proteção, porém, segundo o autor, a mensagem será apreendida como se fosse um mero documento em formato digital, consequentemente, podendo ser apreendida pelas autoridades, nos termos gerais da lei processual penal, não existindo assim qualquer distinção entre mensagem lida ou não lida¹⁹⁷.

No entanto, com a entrada em vigor da Lei do Cibercrime, mais precisamente, com o surgimento do regime da apreensão de correio eletrónico armazenado e registo de comunicação de natureza semelhante, estas posições, defendias antes da sua entrada em vigor, passaram a ter de se ter atenção ao artigo 17.º e à remissão para o artigo 179.º do CPP¹⁹⁸.

Tal como o autor Paulo Pinto de Albuquerque refere, “Deste modo, o legislador optou por equiparar o correio eletrónico ao correio tradicional e abandonar a equiparação às escutas telefónicas que tinha operado no CPP na reforma de 2007.”¹⁹⁹.

Deixou assim de se aplicar ao correio eletrónico previsto no artigo 17.º a extensão legal que está prevista no artigo 189.º, n.º 1 do CPP²⁰⁰.

¹⁹⁵ Neves, Rita Castanheira, ob. cit., p. 183.

¹⁹⁶ Idem, *ibidem*.

¹⁹⁷ Freitas, José Pedro, ob. cit., p. 146.

¹⁹⁸ Albuquerque, Paulo Pinto de, 2023a, p. 792.

¹⁹⁹ Idem, *ibidem*.

²⁰⁰ Mesquita, Pedro Dá, ob. cit., p. 117. “Altera-se nesta norma a matriz adoptada na redacção de 2007 do n.º 1 do art. 189.º do Código de Processo Penal desligando-se, pelo menos parte, do regime do correio electrónico da aplicação, por extensão legal, das regras sobre interceptação de telecomunicações e remetendo-se para as regras sobre apreensão de correspondência que constam do art. 179.º, daquele código.”

Após a entrada em vigor da Lei do Cibercrime, mais precisamente, do seu artigo 17.º, a autora Inês Neves refere que, “(...) o recurso à expressão “armazenados” quer implicar a noção de que o titular já tomou conhecimento do correio electrónico e demais registos, optando por não o eliminar.”²⁰¹.

O outro ponto importante é que alguns autores, tal como Paulo Pinto de Albuquerque, passaram a defender que a aplicação do regime da apreensão de correspondência tem diferenças em termos de regime legal, entre a correspondência física aberta e lida pelo destinatário e o correio eletrónico recebido e lido pelo destinatário, porque após a carta ser recebida torna-se num mero documento, enquanto que o correio eletrónico fica ao abrigo do regime muito mais garantístico da apreensão da correspondência (art. 17.º da Lei do Cibercrime e do art. 179.º do CPP)²⁰².

No entanto, o artigo 17.º não suscita qualquer informação no que toca ao correio eletrónico lido ou não lido pelo seu destinatário, pois pode ser alterado através de um programa que altera o seu estado de lido para não lido²⁰³.

Vamos então passar à análise da nossa jurisprudência, quanto à questão colocada no início deste capítulo: se poderá existir a apreensão da mensagem quando o destinatário não tenha lido tal comunicação?

A nossa jurisprudência distingue a apreensão do correio eletrónico e de SMS fechado e aberto.

Consideramos que se deve abordar não só o correio eletrónico, mas também os SMS, uma vez que o artigo 17.º da Lei do Cibercrime se refere a dados armazenados em suporte digital, resultantes do envio de mensagens do correio eletrónico ou de comunicações de natureza semelhante, resultando assim que as SMS devem ter o mesmo enquadramento legal que as mensagens do correio eletrónico²⁰⁴.

Parte da jurisprudência tem estabelecido a diferenciação entre mensagem aberta e lida e mensagem fechada, ou seja, defendem que depois de recebida e aberta a mesma corresponde a um mero documento, deixando assim de pertencer ao regime das comunicações e gozando da mesma proteção que os documentos, já no caso da

²⁰¹ Neves, Rita Castanheira, ob. cit., p. 276.

²⁰² Albuquerque, Paulo Pinto de, 2023^a, p. 793.

²⁰³ Oliveira, Diogo Castro (2023) – Apreensão de correspondência digital no decurso da pesquisa de dados informáticos, d'Ideias Editora, p. 97.

²⁰⁴ Neste sentido, Gabinete Cibercrime (2020) - Jurisprudência sobre prova digital. Procuradoria-Geral da República. Nota Prática n.º 16/2020, p. 14.

correspondência fechada, esta tem a proteção constitucional que o artigo 34.º n.º 1 da CRP garante ao “sigilo da correspondência”.

Como podemos ver o Acórdão do Tribunal da Relação de Lisboa de 02-03-2011 com o proc. n.º 463/07.3TAALM-A.L1-3, refere que,

Há que distinguir a mensagem já recebida, mas ainda não aberta da mensagem já recebida e aberta.

Na apreensão daquela rege o artigo 179º do CPP, mas a apreensão da já recebida e aberta não tem mais protecção do que as cartas recebidas, abertas e guardadas pelo seu destinatário.

Assim, a correspondência já aberta pelo seu destinatário passa a ter a natureza de documento e goza *apenas* da protecção que todos os documentos merecem.

A correspondência é por definição fechada - assim que é aberta deixa de o ser e passa a ter a natureza documental.

Enquanto fechada, a correspondência é sigilosa por natureza, e, logicamente goza da protecção constitucional que o art. 34.º n.º 1 da Constituição da República Portuguesa concede ao “sigilo da correspondência”²⁰⁵.

Relativamente, à parte onde é referido “Enquanto fechada, a correspondência é sigilosa por natureza, e, logicamente goza da protecção constitucional que o art. 34.º n.º 1 da Constituição da República Portuguesa concede ao “sigilo da correspondência”.”, o Acórdão do Supremo Tribunal de Justiça de 20-09-2006, com o proc. n.º 06P2321, adota uma posição distinta, referindo que a circunstância de as mensagens já terem sido lidas ou não lidas pelo seu destinatário não contribui para esclarecer a questão. Pelo contrário, pode até gerar mais incerteza, uma vez que alguns softwares permitem ao destinatário assinalar uma mensagem como aberta ou fechada, independente de terem mesmo lido ou não, por isso, aquele tem “(...) sempre o direito a não ver essa correspondência que lhe foi endereçada devassada por alguém, sem a sua autorização, constituindo a leitura dessa correspondência intromissão absolutamente ilegítima nela, atentado ao direito à inviolabilidade da mesma, consagrado no art.º 34.º, n.º 4, da CRP”²⁰⁶.

²⁰⁵ Acórdão TRL de 02-03-2011, proc. n.º 463/07.3TAALM-A.L1-3, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d10c400a16882e9e80257853005d65c1?OpenDocument&Highlight=0,463%2F07.3TAALM-A.L1-3>.

²⁰⁶ Acórdão STJ de 20-09-2006, proc. n.º 06P2321, disponível em <https://www.dgsi.pt/jstj.nsf/-/2E7CF04133DD20F78025723D005A62AB>.

Tendo em conta esta defesa, temos de concordar porque não há nada que fundamente esta situação entre o lido e não lido diferentes níveis de proteção jurídica das mensagens de correio eletrónico e comunicações de natureza semelhante²⁰⁷.

Por outro lado, importa referir, que há jurisprudência que defende o contrário, como é o caso do Acórdão do Tribunal da Relação de Lisboa de 15-07-2008 com o proc. n.º 3453/2008-5, que presume que uma vez que a mensagem é recebida em telemóvel é lida pelo seu destinatário, mas faz na mesma a distinção entre mensagem aberta e fechada, afirmando que, “(...) a mensagem mantida em suporte digital depois de recebida e lida terá a mesma protecção da carta em papel que tenha sido recebida pelo correio e que foi aberta e guardada em arquivo pessoal.”²⁰⁸, por isso, explicando por outras palavras, a mensagem uma vez que é aberta e lida passa a ser um mero documento escrito e fica sem proteção da reserva de correspondência e das comunicações.

Tendo em conta a jurisprudência analisada, entendemos que a maior parte utiliza como base nas suas decisões, doutrina anterior a 2007.

No entanto, antes de 2007 não existia de forma expressa “guardadas em suporte digital” ou “armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro” como referência às mensagens de correio eletrónico ou de comunicação de natureza semelhante, pelo que as referidas decisões proferidas pela jurisprudência analisada, não fazem qualquer sentido face ao regime atual, porque a Lei n.º 109/2009 não estabelece a diferença entre a mensagem aberta/lida ou fechada/não lida²⁰⁹, nem o artigo 189.º do CPP e nem a CRP²¹⁰.

²⁰⁷ No mesmo sentido, Cardoso, Rui (2018) - Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX, p. 71, [Consult. 25 nov. 2024]. Disponível em <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30>. ISBN 978-989-8908-17-9.

²⁰⁸ Acórdão TRL de 15-07-2008, proc. n.º 3453/2008-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/9182245992c7c5d18025749000503b8c?OpenDocument&Highlight=0.SMS>.

²⁰⁹ No mesmo sentido, Acórdão STJ de 11-10-2023, proc. n.º 184/12.5TELSB-R.L1-A.S1, disponível em <https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/9b1e715fa7cdbceb80258a4b003f6591?OpenDocument>.

²¹⁰ No sentido do Acórdão TRL de 20-12-2011, proc. n.º 36/11.6PJOER-A.L1-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f1248a82449c5ffd8025798200445cb2?OpenDocument>, “Nem a norma constitucional do art. 34.º n.º 1 da CRP nem as normas processuais penais fazem qualquer distinção entre correspondência fechada e correspondência aberta.

Tal distinção não tem qualquer suporte na letra de lei.

Não há uma diminuição de exigências garantísticas entre correspondência fechada e correspondência aberta.

Independentemente de a correspondência ter sido ou não aberta ou de ter sido ou não lida, a pessoa a quem é dirigida tem sempre o direito de não ver essa correspondência devassada por terceiros.

Por fim, importa referir que como tivemos a oportunidade de analisar, há quem defenda que, uma vez que a mensagem é recebida pelo destinatário, o processo comunicacional termina e deixa de existir qualquer proteção legal²¹¹.

No entanto, como defende Paulo Dá Mesquita, a cessão do ato comunicacional não significa necessariamente “(...) ao fim do âmbito de tutela extensiva do regime das escutas, nomeadamente a exigência de integração num crime de catálogo e a reserva de judicial.”²¹², ou seja, o autor quer dizer que apesar de a mensagem ter sido recebida pelo destinatário não termina a proteção legal. O acesso ou a apreensão da comunicação continua a depender de indícios de crime previstos na lei e da necessidade da autorização judicial.

Noutra perspetiva, alguns autores sustentam que a proteção se mantém até que a mensagem seja efetivamente lida, considerando que o processo comunicacional só fica completo nesse momento, de forma que a mensagem recebida, mas ainda não aberta, estaria ao abrigo do regime da interceção de comunicações²¹³.

Se analisarmos um acórdão mais recente, neste caso, o Acórdão do Supremo Tribunal de Justiça, n.º 10/2023, este clarifica a questão das mensagens abertas ou fechadas. O mesmo refere que,

(...) em síntese conclusiva, que a Lei do Cibercrime criou em relação à apreensão de «correio eletrónico e registos de comunicações de natureza semelhante» um regime específico e unitário, que visou submeter ao regime de apreensão da correspondência, independentemente de as mensagens se encontrarem abertas ou fechadas²¹⁴.

Logo, entende-se que o legislador não especificou que o correio eletrónico tem de estar aberto/fechado ou lido/não lido para se proceder à apreensão da prova digital, por isso, não faz qualquer sentido defender essa distinção de regimes.

Constituindo a leitura da correspondência um atentado ao direito da inviolabilidade da mesma, só o juiz de instrução criminal pode, verificando-se os requisitos legais, determinar a apreensão de correspondência, validar a apreensão de correspondência, ser a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, e, ser quem decide se a mesma é ou não relevante.”

²¹¹ Acórdão TRL de 15-07-2008, proc. n.º 3453/2008-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/9182245992c7c5d18025749000503b8c?OpenDocument&Highlight=0,SMS>.

²¹² Mesquita, Paulo Dá, ob. cit., p. 91.

²¹³ Acórdão TRG de 15-10-2012, proc. n.º 68/10.1GCBRG.G1, disponível em <https://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/d7e67584752588c980257aa0004607b?OpenDocument&Highlight=0,Fernando.monterroso>.

²¹⁴ Acórdão STJ n.º 10/2023, proc. n.º 184/12.5TELSB-R.L1-A.S1, disponível em <https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/10-2023-224081976>.

Porém, todo o tipo de mensagens, independentemente de estarem abertas ou fechadas, estão protegidas pela tutela constitucional do artigo 34.º da CRP, tal como é defendido no acórdão referido anteriormente.

Por sua vez, o artigo 34.º da Constituição, visa proteger o direito fundamental à inviolabilidade do domicílio e da correspondência, ou seja, *prima facie*, a liberdade de manter uma esfera de privacidade e sigilo, livre de interferência e ingerência estadual, quer no que respeita ao domicílio, quer quanto à correspondência, incluindo nesta toda a espécie de correspondência entre pessoas, em suporte físico ou eletrónico²¹⁵.

Contudo, entendemos que a distinção entre mensagem aberta/lida e fechada/não lida não é relevante do ponto vista legal.

A Lei do Cibercrime estabelece dois regimes processuais diferentes (arts. 11.º a 17.º e arts. 18.º a 19.º) que definem a proteção das comunicações de acordo com a forma de acesso à informação, e não segundo o estado de leitura da mensagem²¹⁶.

Mais precisamente, o regime dos artigos 11.º a 17.º trata da apreensão de dados armazenados, incluindo o conteúdo do correio eletrónico. Porém, para se efetuar esta apreensão é sempre necessária a autorização judicial, sob pena de nulidade se não houver exame por parte do JIC (art. 120.º n.º 2 al. d) do CPP)²¹⁷.

O regime dos artigos 18.º e 19.º que regulam a interceção em tempo real, no que toca a dados de tráfego e de conteúdo, ou seja, informações transmitidas durante o processo de comunicação, antes de ficarem armazenadas.

Desta forma, a lei já faz a distinção necessária entre comunicações armazenadas e em trânsito, tornando-se assim irrelevante a diferenciação baseada na mensagem ter sido lida ou não pelo destinatário.

1.1 Tomada de posição

²¹⁵ Acórdão STJ n.º 10/2023, proc. n.º 184/12.5TELSB-R.L1-A.S1, disponível em <https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/10-2023-224081976>.

²¹⁶ Acórdão TRE de 06-01-2015, proc. n.º 6793/11.2DLSB-A.E1, disponível em <https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument&Highlight=0,6793%2F11.2DLSB-A.E1>.

²¹⁷ Nunes, Duarte Rodrigues, (2021), pp. 361 e 362, no mesmo sentido, Venâncio, Pedro Dias, ob. cit., pp. 190 e 191.

De acordo com o artigo 17.º da Lei do Cibercrime, as mensagens armazenadas no sistema informático gozam de proteção constitucional, pelo que é necessária uma autorização judicial para que se possa proceder à apreensão das mesmas.

Portanto, é sempre necessária uma autorização judicial para se proceder à apreensão do correio eletrónico e de registos de comunicação de natureza semelhante para estas possam valer como prova, independentemente, de o destinatário já ter ou não aberto/lido a mensagem.

No mesmo sentido, temos o Acórdão do Tribunal da Relação de Lisboa de 20-12-2011 com o proc. n.º 36/11.6PJOER-A.L1-5, que refere

A jurisprudência e doutrina citadas pelo Mmº JIC, com o devido respeito, pautam-se por uma visão desgarrada dos bens e valores em proteção (a reserva e intimidade da vida privada), plasmados a partir do art.º 34º nº1 da CRP descartando-se destes por via de argumentação centrada no facto de a correspondência estar ou não aberta, o que é completamente irrelevante, pois que o que se pretende é evitar sem controle judicial, em primeira mão, a devassa da vida privada ou segredo profissional inerentes à correspondência apreendida através de acesso por terceiros ou mesmo por intervenientes processuais ao conteúdo daquela.

Esse conteúdo deve ser sempre protegido e garantido, sempre que possível, por prévio controlo judicial.²¹⁸.

Exposto isto, não concordamos em momento algum com as interpretações *contra legem*, que fazem essa distinção. Entendemos que se a própria lei não faz qualquer distinção mais ninguém terá de o fazer.

A norma deve ser aplicada tal como se encontra consagrada na lei, respeitando sempre o que a Constituição prevê e os direitos fundamentais dos cidadãos²¹⁹.

Seguiremos para o último capítulo desta dissertação, que será focado sobre como outros ordenamentos jurídicos, mais precisamente, Alemanha e Espanha, procedem à realização da apreensão do correio eletrónico e de registos de comunicação de natureza

²¹⁸ Acórdão TRL de 20-12-2011, proc. n.º 36/11.6PJOER-A.L1-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f1248a82449c5ffd8025798200445cb2?OpenDocument>.

²¹⁹ Esta exigência significa que não cabe aos intérpretes introduzirem distinções que o nosso legislador não previu (*“ubi lex non distinguit, nec nos distinguere debemus”*).

Apesar de alguns autores sustentarem a diferenciação entre mensagens já abertas e lidas e mensagens ainda fechadas, acabam por atribuir graus de proteção diferentes.

Contudo, a lei não prevê a referida distinção e a própria Constituição no seu artigo 34.º, consagra a inviolabilidade das comunicações em termos gerais, ou seja, abrange igualmente as mensagens lidas e não lidas.

Qualquer diferenciação doutrinária, nesse sentido, implicaria uma restrição contra os direitos fundamentais e à tutela constitucional.

semelhante, sem violarem os direitos fundamentais dos seus cidadãos durante as investigações, relacionando-os com a lei vigente no nosso ordenamento jurídico.

Capítulo 6: O procedimento noutros ordenamentos jurídicos

1. Alemanha

A Lei Fundamental da República Federal Alemã é a sua Constituição (*Grundgesetz*)²²⁰, no seu artigo 10.º faz referência ao sigilo da correspondência, da comunicação postal e da telecomunicação²²¹, que são invioláveis.

No Código Penal Alemão (*Strafgesetzbuch*), mais precisamente, no §202, temos a referência à proteção da correspondência tradicional e no §202a a proibição de acesso a dados por um indivíduo sem autorização, no entanto, na subsecção 2 é definido o conceito de dados, que são os que estão armazenados ou os que são transmitidos eletronicamente, magneticamente ou de outra forma, mas de uma maneira que não seja de imediato perceptível²²².

Já no §206, do mesmo diploma, refere-se à “violação do sigilo do correio ou das telecomunicações”, porém, tipifica o crime quando o agente tem a qualidade de um funcionário ou de um proprietário de um negócio que fornece serviços postais ou de telecomunicações²²³.

Relativamente, ao Código Processual Penal Alemão (*Strafprozeßordnung*), encontramos no §99, a apreensão de correspondência e de telegramas, ou seja, é a norma que permite a apreensão de cartas/postais e telegramas com endereço ao acusado e quando possa existir suspeitas que o conteúdo pode ser importante para a investigação²²⁴.

²²⁰ Para consulta, Deutschland.de [Consult. 10 abril 2025]. Disponível em <https://www.deutschland.de/pt-br/topic/politica/75-anos-da-lei-fundamental-alema>.

²²¹ “(1) O sigilo da correspondência, assim como das comunicações postais e da telecomunicação é inviolável.

(2) Limitações só podem ser ordenadas em virtude da lei.

Se a limitação tiver por finalidade proteger a ordem fundamental livre e democrática ou a existência e segurança da Federação e de um Estado federado, a lei pode determinar que a limitação não seja levada ao conhecimento do indivíduo atingido e que, em vez de se seguir a via judiciária, o controle seja efetuado por órgãos principais e auxiliares, nomeados pelos representantes do povo.” – (2022) - Lei fundamental da República Federal da Alemanha, disponível em <https://www.btg-bestellservice.de/pdf/80208000.pdf>.

²²² Ministro Federal da Justiça [Consult. 10 abril 2025]. Disponível em https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html - p1950.

²²³ Ministro Federal da Justiça [Consult. 10 abril 2025]. Disponível em https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html - p1950.

²²⁴ Para consulta, Strafprozeßordnung (StPO) Código de Processo Penal Alemão, [Consult. 13 abril 2025]. Disponível em https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html - p0557.

No §100, do mesmo diploma, é referido que o tribunal recebe a correspondência fechada, mas para não existir atrasos nas investigações, o mesmo pode transferir a correspondência para o Ministério Público.

Porém, quando o Ministério Público ordenar uma apreensão de correspondência, esta tem de ser aprovada por despacho realizado pelo juiz, no prazo de 3 dias úteis, caso contrário, a dita apreensão é ineficaz.

Segundo o acórdão do Tribunal Constitucional Federal da Alemanha, analisado por Vânia Costa Ramos <<“[a] protecção do segredo das comunicações termina no momento em que a mensagem chega ao destinatário e o processo de transmissão se encontra concluído”>>²²⁵, dá a entender que o sigilo das comunicações protege apenas o trajeto da mensagem até ao destinatário, mas não o seu estado depois de estar na posse do destinatário.

No mesmo acórdão é referido que,

<<“chegados os dados à esfera do recetor, cessa a especial vulnerabilidade ao acesso por terceiros e (...) os dados de ligação e de conteúdo guardados na esfera do recetor deixam de se diferenciar dos dados produzidos pelo próprio.

Enquanto no decurso do processo comunicativo o utilizador não tem possibilidades de impedir a criação e armazenamento dos dados da comunicação, a partir da receção já poderá impedir o acesso aos dados por terceiros, bem como decidir se guarda ou se elimina os dados.

Exceção constitui a interceção de dados no aparelho recetor, se esta for realizada para interceção em tempo real das comunicações.”>>²²⁶.

Do dito até agora podemos retirar que no ordenamento jurídico alemão a apreensão de correio eletrónico não está equiparada à apreensão de correspondência tradicional, tal como acontece em Portugal.

Também se percebe que o segredo das comunicações, neste ordenamento jurídico, tem proteção enquanto a comunicação está em trânsito, e por isso, depois que a mensagem é armazenada, já não existe a dita proteção, tal como acontece no nosso ordenamento jurídico, embora sob regulamentações específicas²²⁷.

²²⁵ Ramos, Armando Dias (2014) – A Prova Digital em Processo Penal, 1ª ed., Chiado Editora, p. 75.

²²⁶ Idem, p. 76.

²²⁷ No mesmo sentido de Armando Dias Ramos, ob. cit. p. 76.

Os métodos de ingerência em comunicações, como meio de obtenção de prova, neste caso, as busca informática remota²²⁸, o legislador alemão preferiu admiti-las em situações onde existem indícios de perigo concreto para vida de uma pessoa e/ou em situações contra a sociedade (os crimes encontram-se expressamente previstos no §100a e no §100b).

No entanto, o §100a e o §100b da StPO, preveem métodos de investigação, nomeadamente, quanto à interceção/registo e pesquisa remota oculta de sistemas de tecnologia da informação, que em ambas as situações não é necessário o conhecimento das pessoas que estão a ser investigadas e em casos urgentes, o Ministério Público pode ordenar as referidas buscas, mas as provas obtidas dessa forma podem tornar-se nulas se num prazo de 3 dias úteis o tribunal não confirmar essas, ou seja, o controlo judicial é obrigatório (§100e, do mesmo diploma).

Em Portugal, como já foi analisado nos capítulos anteriores, é possível a apreensão do correio eletrónico armazenado, prevista nos artigos 179.º do CPP e 17.º da Lei do Cibercrime, tal como a interceção e a gravação de conversações ou comunicações telefónicas (art. 187.º do CPP).

Nas duas é necessária a autorização por despacho por parte do juiz de instrução, sendo que o segundo meio de investigação só pode ser autorizado durante o inquérito e o despacho terá de ser fundamentado, como está previsto no artigo 187.º n.º 1, do CPP.

De igual modo, o artigo 18.º da Lei do Cibercrime prevê a interceção de comunicações em tempo real, aproximando-se do modelo previsto no §100a da StPO. Em Portugal, este meio de obtenção de prova depende sempre de despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, apenas durante o inquérito.

Em contraste, na Alemanha é permitido, que em casos urgentes, seja o Ministério Público a ordenar a interceção, que é sujeita a validação judicial num prazo de 3 dias.

²²⁸ Entende-se por busca informática remota, o acesso direto a computadores ou servidores à distância, no entanto, esta busca é realizada pelas entidades competentes para procurar dados armazenados com o objetivo de apurar a verdade material durante as investigações criminais.

Esta pesquisa é autorizada pela autoridade judiciária.

Em Portugal, também é utilizado este meio de obtenção de prova com as suas diferenças, como é possível ver no Gabinete Cibercrime (2025) – Buscas informáticas (pesquisas) na “CLOUD”. Nota prática n.º 28/2025. Disponível em https://cibercrime.ministeriopublico.pt/sites/default/files/2025-04/cibercrime_nota_pratica_28-2025_02-04-2025.pdf.

Esta diferença demonstra a maior proteção do nosso legislador pela proteção da vida privada e da correspondência dos cidadãos, face à flexibilidade admitida no ordenamento jurídico alemão.

Relativamente, às buscas informáticas remotas, como acontece no ordenamento jurídico alemão, em Portugal, temos dois meios de investigação previstos nos artigos 15.º e 16.º da Lei do Cibercrime que regulam a pesquisa de dados informáticos e a apreensão de dados informáticos.

A pesquisa em sistemas informáticos é realizada em regra no local onde os dados se encontram armazenados, devendo a autoridade judiciária competente, dar a autorização ou ordenar por despacho para que se proceda à dita pesquisa durante um prazo de validade máximo de 30 dias.

Excecionalmente, o OPC pode realizar a pesquisa sem autorização judicial, quando houver consentimento voluntário do titular dos dados ou em casos de terrorismo, criminalidade violenta ou altamente organizada, devendo, nestes casos, a diligência ser posteriormente validada judicialmente e documentada em relatório (art. 253.º do CPP).

Quanto à apreensão de dados, é estabelecido quando necessários à produção de prova, podem ser apreendidos dados ou documentos informáticos, sempre respeitando a validação judicial em prazo máximo de 72 horas.

Em contraste, o ordenamento jurídico alemão permite a realização de buscas informáticas remotas, sem necessidade da polícia se deslocar pessoalmente ao local onde se encontram os dispositivos eletrónicos.

Esta pesquisa remota pode ser efetuada em diversos tipos de crimes graves e não só em situações de terrorismo ou de criminalidade organizada, como acontece em Portugal (§100b do StPO).

Quanto ao correio eletrónico armazenado, pode ser acedido através da busca informática remota, desde que seja autorizado judicialmente pelo tribunal regional onde se encontra o Ministério Público responsável pelo processo (§100e do StPO) ou ser apreendido.

Caso o email esteja em trânsito, este fica ao abrigo do segredo das telecomunicações, onde é necessário pedir a autorização à autoridade judiciária, em caso de urgência o Ministério Público pode dar a ordem.

Exposto isto, é notável que, no nosso ordenamento jurídico, o legislador tenha optado por um modelo mais conservador que o alemão, com respeito ao princípio da legalidade, pela inviolabilidade da vida privada e da correspondência (art. 34.º da CRP) e nesse sentido com a proteção dos direitos fundamentais dos cidadãos.

No que toca ao ordenamento jurídico alemão, o legislador segue um modelo mais flexível, embora seja necessária uma autorização judicial, admite uma maior flexibilidade técnica e de investigação com recursos a instrumentos secretos de recolha de prova digital, através das referidas buscas informáticas remotas, de forma a garantir um equilíbrio entre a eficácia da justiça penal e a proteção dos direitos fundamentais dos seus cidadãos.

2. Espanha

Para finalizar este capítulo, vamos estudar o ordenamento jurídico espanhol e relacionar com o de Portugal.

Em Espanha, a evolução da legislação sobre a matéria do cibercrime foi lenta e marcada por alguma desorganização.

Por se exigir a Lei Orgânica para se proceder à regularização das matérias que prejudiquem os direitos fundamentais e liberdades públicas, o processo legislativo tornou-se mais exigente o que levou ao aumento do tempo e exigindo assim o esforço e o consenso político²²⁹.

Além disso, a Convenção de Budapeste só foi ratificada em 2010, porém, entre 2001 e 2010, foram realizadas adaptações ao ordenamento jurídico de forma progressiva e desarticulada à medida que se transpunham Diretivas ou Decisões-Quadro, aqui destacam se as alterações ao Código Penal pelas leis orgânicas de 15/2003, de 25 de novembro e 5/2010, de 22 de junho, assim como a promulgação da lei 25/2007, de 18

²²⁹ Carvalho, Francisco Proença De, Óscar Morales Garcia e Manuel Álvarez Feijoo (2018) – Regulamentação Supranacional sobre a Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como paradigmas, n.º 48, p. 58 [Consult. 15 abril 2025]. Disponível em <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877> ISSN: 1578-956X.

de outubro, sobre a matéria da conservação de dados relativos às comunicações eletrónicas e às redes públicas de comunicações²³⁰.

Com a ratificação da Convenção e a entrada em vigor da Diretiva 2013/40/UE, de 12 de agosto de 2013, iniciou-se uma nova fase de reformas legislativas em Espanha, alterou-se o Código Penal em 2015 e a Lei Orgânica 13/2015, de 5 de outubro, que introduziu medidas de investigação tecnológica no processo penal²³¹.

Simultaneamente, Espanha adotou a sua Estratégia de Cibersegurança Nacional no final de 2013 e iniciou através do Ministério do Interior, um acompanhamento específico dos dados estatísticos da cibercriminalidade²³².

Por último, a Diretiva 2016/1148, de 16 de julho, foi revogada pela atual Diretiva 2022/2555 do Parlamento Europeu do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de Cibersegurança na União.

No ordenamento jurídico espanhol, o artigo 18.º n.º 3 da Constituição espanhola, protege o segredo das comunicações, mais precisamente, os postais, telegráficas e telefónicas, salvo resolução judicial²³³.

O legislador ainda reforça referindo no n.º 4 do mesmo artigo, que “a lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos.”²³⁴, ou seja, as aplicações das medidas de investigação estarão subordinadas à proteção constitucional da privacidade e limitadas pela lei em questão.

Quanto ao Código Penal Espanhol, apenas existe uma limitação das definições das condutas ilícitas, enquanto no Código de Processo Penal espanhol, consta a

²³⁰ Carvalho, Francisco Proença De, Óscar Morales Garcia e Manuel Álvarez Feijoo (2018) – Regulamentação Supranacional sobre a Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como paradigmas, n.º 48, p. 58 [Consult. 15 abril 2025]. Disponível em <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877> ISSN: 1578-956X.

²³¹ Carvalho, Francisco Proença De, Óscar Morales Garcia e Manuel Álvarez Feijoo (2018) – Regulamentação Supranacional sobre a Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como paradigmas, n.º 48, p. 58 [Consult. 15 abril 2025]. Disponível em <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877> ISSN: 1578/956X.

²³² Carvalho, Francisco Proença De, Óscar Morales Garcia e Manuel Álvarez Feijoo (2018) – Regulamentação Supranacional sobre a Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como paradigmas, n.º 48, p. 58 [Consult. 15 abril 2025]. Disponível em <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877> ISSN: 1578/956X.

²³³ Constitución Española, [Consult. 15 abril 2025]. Disponível em <https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugués.pdf>.

²³⁴ Constitución Española, [Consult. 15 abril 2025]. Disponível em <https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugués.pdf>.

regulamentação detalhada dos procedimentos quanto à interceção e apreensão de comunicações eletrónicas e é esta parte a que iremos dar destaque.

Relativamente ao Código de Processo Penal Espanhol (*Ley de Enjuiciamiento Criminal*), está consagrado todas as medidas de investigação para a obtenção de prova, desde o artigo 545.º a 588.^{o235}.

No que toca à apreensão e abertura da correspondência tradicional, está previsto nos artigos 579.º a 588.º, mais precisamente, o artigo 580.º que prevê as regras a aplicar em caso de apreensão de correspondência tradicional, porém, o juiz é que decide se pode proceder à apreensão ou não, ou seja, caso haja indícios que poderão ajudar para a descoberta da verdade (art. 579.º do mesmo diploma).

No capítulo IV ao capítulo IX do referido diploma, está consagrado as disposições comuns à interceção das comunicações telefónicas e telemáticas, ao registo e gravação de comunicações orais através da utilização de dispositivos eletrónicos, à utilização de dispositivos técnicos de rastreamento, localização e registo de imagens, ao registo de dispositivos de armazenamento em massa de informação e aos registos remotos sobre equipamentos informáticos.

Nos termos dos artigos 588.º *ter a.* a 588.º *ter i.*²³⁶, está prevista a possibilidade da interceção de comunicações telefónicas e telemáticas, sempre que a comunicação estiver em trânsito, ou seja, por exemplo, as mensagens que ainda não tenham sido recebidas pelo seu destinatário, porém, tem de existir um pedido de autorização judicial com os respetivos requisitos.

Nos casos de urgência (terrorismo ou criminalidade organizada), a competência cabe ao Ministro do Interior ou ao Secretário de Estado da Segurança, mas o juiz tem de dar a autorização de forma fundamentada em 72 horas, tal como consta no artigo 588.º *ter d.* n.º 3, do mesmo diploma.

Por outro lado, quando a mensagem ou outras formas de comunicação já se encontram armazenadas no dispositivo do destinatário (telemóvel, computador, etc..), aplica-se o regime do registo remoto de equipamentos informáticos, previsto nos artigos 588.º *septies a.* a 588.º *septies c.*, que permite, mediante autorização judicial, o acesso de forma remota e telemática, o exame à distância e sem o conhecimento do seu titular do

²³⁵ Ley de Enjuiciamiento Criminal, [Consult. 18 abril 2025]. Disponível em <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036-a584>.

²³⁶ Ley de Enjuiciamiento Criminal, [Consult. 18 abril 2025]. Disponível em <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&p=20250103&tn=2>.

conteúdo do dispositivo eletrónico, através da instalação de um software e também do uso de dados de identificação e códigos.

Para tal procedimento, apenas será em situações que estão previstas no artigo 588.º *septies* a. n.º 1: a) crimes cometidos em seio de organizações criminosas; b) crimes de terrorismo; c) crimes cometidos contra menores ou pessoas com capacidade judicialmente modificada; d) crimes contra a Constituição, de traição e relativos à defesa nacional; e) crimes cometidos através de instrumentos informáticos ou de qualquer outra tecnologia da informação ou telecomunicações ou serviço de comunicação²³⁷.

Tendo em conta a análise do ordenamento jurídico de Espanha percebemos que existem parecenças com o regime jurídico de Portugal, mais precisamente, quanto à necessidade de controlo no acesso e à apreensão de comunicações eletrónicas, mas também diferenças em relação aos procedimentos e às exceções.

Em Portugal, o procedimento rege-se de uma forma mais rígida, ou seja, exige-se sempre um despacho judicial prévio para a apreensão de correio eletrónico armazenado e de registo de comunicação de natureza semelhante, nos termos do artigo 17.º da Lei do Cibercrime, em conjugação com o artigo 179.º do CPP e também é necessário um despacho fundamentado pelo juiz e mediante requerimento do Ministério Público para a interceção e a gravação de comunicações telefónicas ou outras formas de transmissão de dados por via telemática (art. 187.º a 189.º, do CPP e art. 18.º da Lei do Cibercrime).

No entanto, não existem exceções que permitam a intervenção do Ministério Público sem autorização judicial, mesmo em casos de terrorismo ou de criminalidade organizada, ao contrário do que acontece em Espanha, que prevê exceções em caso de urgência.

Exposto isto, tal como acontece no ordenamento jurídico da Alemanha, em Espanha não é muito diferente, ambos têm normas mais flexíveis para casos de urgência para a proteção dos cidadãos e para garantir um equilíbrio na proteção dos direitos fundamentais, já em Portugal, opta-se por um modelo mais restrito para a proteção dos direitos fundamentais, deixando sempre o juiz como garante da legalidade e com o cumprimento do princípio da proporcionalidade.

No entanto, consideramos que Portugal pode aperfeiçoar e implementar algumas normas inspirando-se nestes ordenamentos jurídicos, desde logo, adotar o regime que

²³⁷ Ley de Enjuiciamiento Criminal, [Consult. 19 abril 2025]. Disponível em <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&p=20250103&tn=1 - cv-6>.

eles adotam em situações de urgência e a possível implementação de normas no que toca às buscas informáticas remotas em crimes graves e não só em casos de terrorismo ou criminalidade organizada, sem deixar de garantir o controlo judicial e o respeito pelos direitos fundamentais dos cidadãos.

Conclusão

A presente dissertação teve como objetivo analisar, de forma aprofundada e crítica, o procedimento de apreensão do correio eletrónico armazenado e dos registos de comunicação de natureza semelhante, tendo como base o regime consagrado no artigo 17.º da Lei do Cibercrime, como também perceber a sua articulação com o Código Processual Penal e a Constituição da República Portuguesa.

Num primeiro momento, foi importante clarificar o conceito de prova digital e dos demais conceitos com ela relacionados de forma a perceber a sua importância e a adaptação do sistema jurídico português às novas realidades tecnológicas que estão sempre em evolução. Assim desenvolveu-se o conceito de correio eletrónico que consiste num meio de comunicação rápido entre duas ou mais pessoas que pode ser utilizado para enviar imagens, mensagens escritas e por voz.

Também no que toca à questão do correio eletrónico, frisamos a distinção entre as mensagens enviadas e recebidas e a este propósito abordamos o problema das mensagens instantâneas que são caracterizadas pela facilidade e a rapidez na comunicação e onde foi destacado o problema da encriptação de ponta-a-ponta que garante uma maior proteção e privacidade e ao mesmo tempo uma acrescida dificuldade no que tange às investigações realizadas pelas autoridades.

Também se distinguiu as mensagens abertas/lidas e fechadas/não lidas e demonstrou-se que esta distinção tem uma relevância prática e jurídica, refletindo-se diretamente nos procedimentos de apreensão e na sua admissibilidade como meio de prova, evidenciado as diferenças essenciais entre as comunicações *online* e a correspondência tradicional.

Também se falou das comunicações de natureza semelhante ao correio eletrónico, que são as referidas mensagens instantâneas que podem ser enviadas por voz, texto ou imagens, através da Internet pelas aplicações do Messenger, WhatsApp, Skype, Viber, Snapchat, Telegram, Facebook, entre outros.

Passamos de seguida à análise da evolução legislativa e tal permitiu perceber que Portugal harmonizou a sua legislação aos regulamentos internacionais, em especial à Convenção de Budapeste, à Decisão-Quadro 2005/222/JAI do Conselho da União

Europeia e à Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

Estes diplomas demonstram o esforço da União Europeia em criar uma resposta coordenada face à criminalidade informática, impondo também aos ordenamentos jurídicos nacionais a obrigação de adaptar normas processuais à nova realidade digital.

Num terceiro momento, procedemos finalmente à análise do artigo 17.º da Lei do Cibercrime, que consagra o regime da apreensão do correio eletrónico e de registos de comunicação de natureza semelhante que se encontram armazenados no sistema informático e foi entendido que quando o juiz autorizar ou ordenar, por despacho a dita apreensão é que as autoridades podem atuar e obter a informação que se revela importante para a descoberta da verdade material ou para a prova²³⁸.

Relativamente à lista de crimes que permitem a apreensão de correio eletrónico e de comunicações análogas, foi esclarecido que não existe qualquer lista, pois se encontram espalhados em legislação avulsa e pelo Código Penal.

Quanto à remissão para o artigo 179.º do Código de Processo Penal, revelou-se um dos aspetos mais debatidos nesta dissertação e concluímos que a referida remissão para o regime da correspondência deve ser lida de forma ajustada ao correio eletrónico, sob pena de se aplicar um regime concebido para a correspondência física a uma realidade imaterial, assim, defendeu-se, com apoio de diversos autores, que o correio eletrónico não deve ser equiparado a uma carta tradicional, precisamente por não partilharem a mesma natureza material nem o mesmo circuito de transmissão/entrega.

No que toca à atuação das autoridades, que utilizam este meio de obtenção de prova previsto no artigo 17.º da Lei do Cibercrime, reforçou-se a importância de respeitar o princípio do acusatório consagrado no artigo 32.º, n.º 5 da Constituição da República Portuguesa, segundo o qual o Ministério Público, como titular da ação penal e entidade que dirige a fase de inquérito, deve dispor da autonomia para proceder à recolha de prova, apesar de ser sempre sujeito ao controlo judicial.

Assim, sustentou-se que não se justifica impor ao juiz de instrução criminal o ónus de ser a primeira pessoa a tomar conhecimento do conteúdo de todas as mensagens

²³⁸ Quanto às interceções em tempo real só referimos que ficam ao abrigo do artigo 18.º da Lei do Cibercrime, pois o legislador teve a preocupação de diferenciar os dois momentos da comunicação, garantindo um equilíbrio entre a realização da investigação e o respeito pelos direitos fundamentais.

apreendidas, porque este último ao permitir que aquelas possam ser apreendidas, garante que não irá existir violação dos direitos fundamentais, desde logo, um dos seus deveres é garantir que nenhum dos direitos, liberdades e garantias sejam violados durante as investigações realizadas pelo Ministério Público.

Nos casos de *periculum in mora*, isto é, quando exista fundado receio de que o decurso do tempo possa comprometer a eficácia da apreensão ou fazer desaparecer a prova digital armazenada, foi considerado que se justifica nestes casos que os órgãos de polícia criminal, pratiquem medidas cautelares urgentes, e por isso, sem autorização prévia do juiz de instrução criminal, desde que tal atuação seja convalidada por despacho fundamentado do juiz num prazo de quarenta e oito horas.

O artigo 17.º da Lei do Cibercrime remete para o artigo 179.º do CPP, sem estabelecer qualquer exigência expressa quanto ao grau de suspeita necessário para se recorrer a este meio de obtenção de prova. Porém, em respeito ao princípio da proporcionalidade e à proteção da esfera íntima consagrada constitucionalmente, entende-se que, quando os dados incidam sobre a vida privada, deve ser exigida uma suspeita fundada.

Quanto à denúncia anónima, pode desencadear a abertura do inquérito como também irá permitir a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante desde que esteja ao abrigo do artigo 246.º, n.º 6 do CPP. A relevância jurídica da denúncia cabe sempre ao Ministério Público apreciar, podendo conduzir à sua utilização processual ou à sua destruição, consoante a fase processual em que surja e a existência ou não, de indícios da prática de crimes.

Num quarto momento, ficou esclarecido que o procedimento da apreensão do artigo 17.º da Lei do Cibercrime exige uma leitura cuidada à luz dos direitos fundamentais que estão consagrados na Constituição da República Portuguesa.

Desde logo, analisou-se o direito à reserva da vida privada, consagrado no artigo 26.º e o direito à inviolabilidade da correspondência e das comunicações, prevista no artigo 34.º, como os mais relevantes quando estão em causa estes meios de obtenção de prova, pois à luz destes direitos o conteúdo das mensagens estará sempre protegido e mesmo quando se proceder a uma apreensão desse conteúdo tal terá de ter que em consideração o princípio da proporcionalidade de forma a não existir decisões injustas e que violem os direitos, liberdades e garantias dos cidadãos.

A análise feita permitiu ainda perceber que, no caso do correio eletrónico, mesmo estando armazenado tem proteção constitucional, mas não tem a mesma proteção da palavra falada em tempo real.

Por outro lado, salientou-se a diferença entre a proteção de dados pessoais segundo a Carta dos Direitos Fundamentais da União Europeia, no seu artigo 8.º e a privacidade prevista no artigo 8.º da Convenção Europeia dos Direitos Humanos.

O primeiro artigo consagra de forma mais específica a proteção de dados pessoais dentro da União Europeia, enquanto o segundo artigo prevê o tema da privacidade num sentido mais amplo, ou seja, na proteção da vida privada, neste caso, da correspondência, porém ambos garantem uma proteção contra as violações praticadas durante as investigações criminais, mais precisamente, das apreensões do correio eletrónico e comunicações análogas.

No Capítulo 5, foi analisado o tratamento jurisdicional da apreensão do correio eletrónico e dos registos de comunicação de natureza semelhante e foi possível ver que continua a gerar interpretações diferentes, sobretudo quanto à distinção entre o correio aberto e fechado.

A posição adotada sustenta que o artigo 17.º da Lei do Cibercrime não distingue entre mensagens lidas ou não lidas, não devendo a jurisprudência nem a doutrina criar uma distinção que a lei não faz.

Neste estudo evidenciou-se também que enquanto a correspondência tradicional deixa de estar protegida pelo segredo das comunicações logo após a sua abertura realizada pelo destinatário, o mesmo raciocínio não pode ser aplicado quanto ao correio eletrónico, dada à sua natureza imaterial, é possível ser armazenado, e facilmente recuperável mesmo após ser lida.

A jurisprudência e a doutrina ainda não chegaram a um consenso, no entanto, defendeu-se que não faz sentido insistir numa equiparação entre o correio eletrónico e a correspondência tradicional, já que cada um apresenta características próprias que exigem uma interpretação diferente.

Independentemente das divergências conclui-se que as autoridades judiciais devem assegurar que qualquer apreensão de comunicações digitais seja necessária, proporcional, tendo sempre em vista a descoberta da verdade material.

A análise comparativa com os ordenamentos jurídicos da Alemanha e de Espanha permitiu perceber como procedem relativamente à apreensão do correio eletrónico e de registos de comunicação de natureza semelhante.

Esta comparação demonstrou que no ordenamento jurídico português, apesar de ter um regime justo de apreensão de correio eletrónico armazenado e registos de comunicação de natureza semelhante consagrado na Lei do Cibercrime e no Código de Processo Penal, existe ainda espaço para aperfeiçoamentos inspirados nestes dois ordenamentos jurídicos, nomeadamente quanto a buscas informáticas remotas (em Portugal, “pesquisa de dados informáticos”) e em situações de urgência.

Embora em situações *periculum in mora* já seja possível no ordenamento jurídico português haver intervenção imediata do OPC sem prévia autorização da autoridade judiciária (art. 15.º, n.º 3, da Lei do Cibercrime), a atuação continua a ser mais restrita do que nos ordenamentos jurídicos abordados e não admite a mesma flexibilidade no regime.

Em suma, a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante continuará a ser um tema de grande relevância, num contexto em que a tecnologia está sempre em processo de desenvolvimento a um ritmo acelerado, criando outras formas de comunicação e outras oportunidades, mas também irá trazer novos riscos para a criminalidade que terão de ser resolvidos.

Espera-se que esta dissertação possa contribuir para uma aplicação mais clara, coerente e equilibrada das normas vigentes, estimulando à reflexão crítica e promovendo o equilíbrio sempre indispensável entre a eficácia da justiça penal e a proteção dos direitos fundamentais dos cidadãos.

Bibliografia

Albuquerque, Paulo Pinto de (org.) (2019) – Comentário da Convenção dos Direitos Humanos e dos Protocolos Adicionais, Volume II, Universidade Católica Editora;

Albuquerque, Paulo Pinto de (2023) – Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos, Volume I, 5ª ed., Universidade Católica Editora;

Albuquerque, Paulo Pinto de (2023) – Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos Humanos, Volume II, 5ª ed., Universidade Católica Editora;

Bravo, Rogério (2006) – Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta. Revista Polícia e justiça, Instituto Superior de Polícia Judiciária e de Ciências Criminais III Série, n.º 7, Coimbra Editora;

Canotilho, José Joaquim Gomes e Vital Moreira (2007) – Constituição da República Portuguesa Anotada, vol. I, 4ª ed., Coimbra Editora;

Canotilho, José Joaquim Gomes e Vital Moreira (2010) – Constituição da República Portuguesa Anotada, Vol. II, 4ª ed., Coimbra Editora;

Cardoso, Rui (2018) - Apreensão do correio electrónico e registos de comunicações de natureza semelhante – Artigo 17º da Lei n.º 109/2009, de 15.IX. Disponível em [https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30.](https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U=&portalid=30;);

Carvalho, Francisco Proença De, Óscar Morales Garcia e Manuel Álvarez Feijoo (2018) – Regulamentação Supranacional sobre a Criminalidade Informática e Técnicas de Transposição. O Direito Penal Português e Espanhol como Paradigmas, n.º 48. Disponível em <https://www.uria.com/documentos/publicaciones/5801/documento/art04.pdf?id=7877>, ISSN: 1578-956X;

Comissão Nacional de Proteção de Dados (CNPd). Disponível em <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>;

Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões (2015) – Rumo a uma política geral de luta contra o cibercrime. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3A14560&qid=1736473558179>;

Conselho Europeu / Conselho da União Europeia (2024) – Regulamento Geral Sobre a Proteção de Dados. Disponível em <https://www.consilium.europa.eu/pt/policies/data-protection/data-protection-regulation/>;

Constitución Española. Disponível em <https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugués.pdf>;

Convenção Europeia dos Direitos do Homem. Disponível em https://www.echr.coe.int/documents/d/echr/convention_por;

Correia, João Conde, et. al. (2020) – Comentário Judiciário do Código Processo Penal, Tomo II, Artigos 124º a 190º, 2ª ed., Almedina Editora;

Costa, José Faria (1998) – Direito Penal da Comunicação (Alguns escritos), Coimbra Editora;

Deutschland.de. Disponível em <https://www.deutschland.de/pt-br/topic/politica/75-anos-da-lei-fundamental-alema>;

Diário da República. Disponível em <https://diariodarepublica.pt/dr/lexionario/termo/crime-particular>,

Diário de notícias, disponível em <https://www.dn.pt/sociedade/europol-declara-guerra-as-mensagens-encryptadas-que-travam-investigacoes-pj-juntou-se-ao-alerta>;

EU Innovation Hub (2024) – First Report on Encryption. Disponível em https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First_Report_on_Encryption.pdf;

EUR-Lex – Access to European Union law, CDFUE. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12016P%2FTXT>;

EZTALKS – Mensagens instantâneas. Disponível em <https://pt.eztalks.com/unified-communications/8-examples-of-instant-messaging.html> - google_vignette;

Fernandes Soares, Paulo Alexandre (2017) – Meios de Obtenção de Prova no Âmbito das Medidas Cautelares e de Polícia, 2ª ed., Almedina Editora;

Fichas temáticas sobre União Europeia – 2025, disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf;

Figueiredo Dias, Jorge de (2024) – Direito Processual Penal. Estudos, 1ª ed., Gestlegal Editora;

Freitas, José Pedro (2020) – Os meios de obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos serviços de Correio Eletrónico e de Mensagens Curtas, Nova Causa Editora;

Gabinete Cibercrime (2020) – Jurisprudência sobre prova digital. Procuradoria geral da República, Nota Prática n.º 16/2020;

Gabinete Cibercrime (2025) - Buscas informáticas (pesquisas) na “CLOUD”. Nota prática n.º 28/2025. Disponível em https://cibercrime.ministeriopublico.pt/sites/default/files/2025-04/cibercrime_nota_pratica_28-2025_02-04-2025.pdf;

IBM – O que é a criptografia de ponta a ponta (E2EE)? Disponível em <https://www.ibm.com/br-pt/topics/end-to-end-encryption>;

Jornal Oficial da União Europeia. Disponível em <https://op.europa.eu/pt/publication-detail/-/publication/708d86d8-ab9a-4e18-9bda-ac37405a3185>;

Kaspersky – Endereço IP. Disponível em <https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address>;

Lei Fundamental da República Federal da Alemanha. Disponível em <https://www.btg-bestellservice.de/pdf/80208000.pdf>;

Ley do Enjuiciamiento Criminal. Disponível em <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036-a584>;

Malwarebytes – Phishing. Disponível em <https://www.malwarebytes.com/pt-br/phishing>;

Mesquita, Pedro Dá (2010) – Processo Penal, Prova e Sistema Judiciário, 1ª ed., Coimbra Editora;

Ministério Público – Consulta de tratados internacionais. Convenção sobre o Cibercrime. Disponível em <https://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0>;

Ministério Público – Portugal. Disponível em <https://www.ministeriopublico.pt/perguntas-frequentes/crime>;

Ministério Público – Procuradoria-Geral Regional de Lisboa. Lei n.º 79/2021, de 24 de novembro. Para consulta, disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3476&tabela=leis&ficha=1&pagina=1&so_miolo=;

Ministro Federal da Justiça. Disponível em https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html-p1950;

Minuta de Relatório Explicativo, disponível em <https://rm.coe.int/16802fa429>;

Neves, Inês Castanheira (2011) – As Ingerências nas Comunicações Eletrónicas em Processo Penal, 1ªed., Coimbra Editora;

Nunes, Duarte Rodrigues (2019) – O problema da admissibilidade dos métodos “ocultos” de investigação criminal como instrumento de resposta à criminalidade organizada, 1ª ed., Gestlegal Editora;

Nunes, Duarte Rodrigues (2021) – Os meios de obtenção de prova previstos na Lei do Cibercrime, 2ª ed., Gestlegal Editora;

Nunes, Duarte Rodrigues (2023) – Curso de Direito Processual Penal – Tomo II, Elementos do processo penal (continuação). O procedimento criminal. Universidade Católica Editora;

Oliveira, Diogo Castro (2023) – Apreensão de correspondência digital no decurso da pesquisa de dados informáticos, d'Ideias Editora;

Ramos, Armando Dias (2014) – A Prova Digital em Processo Penal, 1ª ed., Chiado Editora;

Relatório Explicativo da Convenção do Conselho da Europa para a Proteção das crianças contra a Exploração Sexual e aos Abusos Sexuais (2020) - Lanzarote, 25.X.2007. Disponível em https://dgpj.justica.gov.pt/Portals/31/Edi%E7%F5esDGPJ/REL_EXP.pdf;

Schwalbach, José Gaspar (2021) – Direito Digital, 2ª ed., Almedina Editora;

Scientia IVRIDICA (2009) - Pedro Verdelho – A nova Lei do Cibercrime, Tomo LVIII – N.º 320;

Strafprozeßordnung (StPO) Código de Processo Penal Alemão. Disponível em https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html - p0557;

TWILIO – Mensagens. Disponível em <https://www.twilio.com/pt-br/resource-center/what-are-sms-and-mms>;

Venâncio, Pedro Dias (2023) – Lei do Cibercrime, Anotada e Comentada, Atualizada pela Lei n.º 79/2021, de 24 de novembro, Coimbra d'Ideias Editora;

Verdelho, Pedro (2004) - Apreensão de correio electrónico em Processo Penal. Ministério Público, ano 25, n.º 100. Disponível em https://rmp.smppt.pt/ermp/rmp_100/mobile/index.html - p=74;

Jurisprudência

Tribunal da Relação de Lisboa:

Acórdão do Tribunal da Relação de Lisboa de 10-08-2020, proc. n.º 6330/18.8JFLSB-A.L1-3, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8ce57ecb0a16a8e0802585ec0036019a?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 20-12-2011, proc. n.º 36/11.6PJOER-A.L1-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f1248a82449c5ffd8025798200445cb2?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 02-03-2011, proc. n.º 463/07.3TAALM-A.L1-3, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d10c400a16882e9e80257853005d65c1?OpenDocument&Highlight=0,463%2F07.3TAALM-A.L1-3>;

Acórdão do Tribunal da Relação de Lisboa de 02-05-2023, proc. n.º 12234/21.0T8LSB.L1-7, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6b57c49941d5779f802589aa0049be2a?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 11-07-2019, proc. n.º 184/12.5TELSB-B.L1-3, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1bc410315a7483298025843b004c1e71?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 24-09-2013, proc. n.º 145/10.9GEALM.L2-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c60dfe830c97cf8980257c0000368afa?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 11-01-2011, proc. n.º 5412/08.9TDLSB-A.L1-5, disponível em [https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument&Highlight=0,apreensão,correspondência](https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument&Highlight=0,apreensão,correspondência;);

Acórdão do Tribunal da Relação de Lisboa de 06-02-2018, proc. n.º 1950/17.0T9LSB-A.L1-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 09-06-2016, proc. n.º 50/14.0SLLSB-Y.L1-9, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8cf93372a59dc58480257fd3004a5256?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 07-03-2018, proc. n.º 184/12.5TELSB-B.L1-3, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 05-05-2022, proc. n.º 305/19.7T9AGH-A.L1-9, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/97c0f4f65870d61e80258847003929a9?OpenDocument>;

Acórdão do Tribunal da Relação de Lisboa de 11-05-2023, proc. n.º 215/20.5T9LSB-C.L1-9, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/650a771605b574f6802589b2004bc175?OpenDocument&Highlight=0,n.º,215%2F20.5T9LSB-C.L1-9>;

Acórdão do Tribunal da Relação de Lisboa de 15-07-2008, proc. n.º 3453/2008-5, disponível em <https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/9182245992c7c5d18025749000503b8c?OpenDocument&Highlight=0,SMS>

Tribunal da Relação de Guimarães:

Acórdão do Tribunal da Relação de Guimarães de 15-10-2012, proc. n.º 68/10.1GCBRG.G1, disponível em <https://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/d7e67584752588c980257aa0004607bc?OpenDocument&Highlight=0,Fernando,monterroso>;

Tribunal da Relação de Évora:

Acórdão do Tribunal da Relação de Évora de 06-01-2015, proc. n.º 6793/11.2TDLSB-A.E1, disponível em <https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument&Highlight=0,6793%2F11.2TDLSB-A.E1>;

Supremo Tribunal de Justiça:

Acórdão do Supremo Tribunal de Justiça de 11-10-2023, proc. n.º 184/12.5TELSB-R.L1-A.S1, disponível em <https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/9b1e715fa7cdbceb80258a4b003f6591?OpenDocument>;

Acórdão do Supremo Tribunal de Justiça de 20-09-2006, proc. n.º 06P2321, disponível em <https://www.dgsi.pt/jstj.nsf/-/2E7CF04133DD20F78025723D005A62AB>;

Tribunal Constitucional:

Acórdão do Tribunal Constitucional n.º 219/89, proc. n.º 324/88, disponível em <https://www.tribunalconstitucional.pt/tc/acordaos/19890219.html>;

Acórdão do Tribunal Constitucional n.º 314/2023, proc. n.º 145/2021, disponível em <https://www.tribunalconstitucional.pt/tc/acordaos/20230314.html>;

TEDH:

Acórdão do TEDH Laurent C. França – 28798/13, de 24-05-2018, disponível em [https://hudoc.echr.coe.int/fre - {"itemid":\["001-183129"\]}](https://hudoc.echr.coe.int/fre - {);

TJUE:

Acórdão do TJUE de 07-03-2024, proc. n.º C-604/22, disponível em <https://curia.europa.eu/juris/document/document.jsf?text=&docid=283529&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=1203>.