



UNIVERSIDADE D
COIMBRA

Jéssica Beatriz Marques Morim

**APREENSÃO DE MENSAGENS DE CORREIO
ELETRÓNICO E A TEMÁTICA DOS CONHECIMENTOS
FORTUITOS**

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses, orientada
pela Professora Doutora Sónia Mariza Florêncio Fidalgo e apresentada à
Faculdade de Direito da Universidade de Coimbra

Julho de 2022



FACULDADE DE DIREITO
UNIVERSIDADE DE
COIMBRA

Jéssica Beatriz Marques Morim

**Apreensão de Mensagens de Correio Eletrónico e a Temática dos Conhecimentos
Fortuitos**

The Seizure of Electronic Mail Messages and the Thematic of Random Knowledge

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do
2º Ciclo de Estudos em Ciências Jurídico-Forenses (conducente ao grau de Mestre)

Orientadora: Professora Doutora Sónia Mariza Florêncio Fidalgo

Coimbra, 2022

AGRADECIMENTOS

*Aos meus pais e irmãos pelo apoio e amor incondicional,
Aos meus avós maternos e paternos e outros entes queridos, que me observam do Paraíso,
À Faculdade de Direito da Universidade de Coimbra, que contribuiu para o meu
enriquecimento pessoal e académico,
À minha orientadora, Professora Doutora Sónia Fidalgo, pelo auxílio concedido durante
este período,
Às minhas amigas e amigos de Pombal e Coimbra,
Aos que por mim passaram e nos quais deixei a minha marca,
A Coimbra, cidade que me viu nascer, que me acolheu durante seis anos e que me
acompanhará para o resto da vida.*

RESUMO E PALAVRAS-CHAVES

O corpo da dissertação propriamente dito inicia-se com a análise dos diplomas internacionais, cuja combinação culminou na Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro. De imediato, torna-se imperioso, não só tomar conhecimento da constituição da mesma, de forma a contextualizar a apreensão de mensagens de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17º da LC), como também problematizar a consagração da LC enquanto lei extravagante. O escrutínio relativo ao âmbito de aplicação (artigo 11º, n.º 1 da LC) possibilita o conhecimento de quais as realidades em que será conveniente mobilizar a LC, nomeadamente os meios processuais direcionados para a obtenção de prova em ambiente digital. Posteriormente, o estudo versará sobre a discussão que se colocou com a entrada em vigor da LC e com a alteração introduzida no artigo 189º do CPP, pela Lei n.º 48/2007, de 29 de agosto. Segundo este artigo aplicar-se-á o regime previsto nos artigos 187º e 188º do CPP. É imperativo a determinação do regime a aplicar, a fim de proporcionar a maior e melhor salvaguarda dos direitos fundamentais dos envolvidos. Como tal é essencial delimitar o conjunto dos direitos fundamentais restringidos.

Para proporcionar o paralelismo desejado, entre a apreensão de correio eletrónico e as escutas telefónicas torna-se indispensável a abordagem de problemáticas associadas ao regime exposto no artigo 17º da LC, nomeadamente a necessidade de diferenciação entre mensagens de correio eletrónico fechadas/não lidas e abertas/lidas; a exigibilidade do despacho judicial prévio a autorizar a apreensão; que o juiz de instrução seja o primeiro a tomar conhecimento das mensagens e, finalizando, que o tipo de ilícito possua uma moldura penal, cuja pena de prisão é, no seu máximo, superior a 3 anos.

Por sua vez, com a finalidade de conhecer da admissibilidade da valoração de mensagens de correio eletrónico, num processo diverso daquele em que teve origem a respetiva valoração, é obrigatório conhecer da distinção entre conhecimentos fortuitos e conhecimentos de investigação; o percurso que a doutrina e a jurisprudência efetuaram, num momento em que a lei não estipulava qualquer norma quanto à respetiva admissibilidade no seio das escutas telefónicas e os requisitos impostos pelo legislador ordinário, no artigo 187º, n.º 7 do CPP, aquando da consagração. Terminarei a abordagem com o raciocínio estabelecido, para concluir sobre a valoração dos conhecimentos fortuitos no segundo

processo, no seguimento da apreensão de correspondência eletrónica, no seio de processo diverso.

Palavras-Chave: Lei do Cibercrime; Apreensão; Correio eletrónico; Registos de comunicações de natureza semelhante; Escutas telefónicas; Conhecimentos de investigação e conhecimentos fortuitos.

ABSTRACT

The dissertation body itself begins with the analysis of some international diplomas, which lead to the Cybercrime Law, n.º 109/2009, of 15 of September. Therefore, it is truly important not only to know its constitution, to contextualize the seizure of electronic e-mail and communication records of a similar nature, provided in article 17 of the LC, but also to question why it was enshrined as an extravagant law. The scrutiny concerning the scope of the application (article 11, n.º 1 of the LC), allows us to understand which realities should be considered for the LC, especially the processual ways used on the collection of evidence in a digital context.

After, this study will talk about the discussion which came with the entry into force of the LC and with the amendment introduced by Law n.º 48/2007, of 29 of August, in which the application of the legal regime of the articles 187 and 188 of the CPP is mentioned in article 189. In fact, it is necessary to determine which regime should apply to ensure the safeguard of the citizens' rights as it is essential to delimit the set of fundamental rights which are being restricted.

To provide the parallelism between the seizure of electronic mail and the wiretapping, it is crucial to mention the problematics under article 17 of the LC regime, mostly the need to distinguish between closed mail/unread mail and opened mail/read mail; the obligation of the preview court order which will authorize the seizure, so that the instruction judge will be the first one to appreciate the content of the messages; and, finally, that the specific crime has a penalty frame, whose prison sentence is, in its maximum, more than 3 years.

To ascertain the admissibility of valuation of electronic mail messages, in different processes, of the one in which it was originated its valuation, it is imperative to understand the differences between random knowledge and research knowledge. Besides that, it is also important to understand the path that doctrine and jurisprudence have taken before the stipulation of any rules by the Law, regarding the admissibility at wiretapping and the legislator's requirements, in article 187, n.º 7 article of the CPP. The analysis will be concluded with the reasoning made, to conclude about de valuation of random knowledge, in the second process, following the seizure of electronic mail, in another process.

Keywords: Cybercrime Law; Seizure; Electronic mail; Communication of similar nature; Wiretapping; Random knowledge; Research knowledge

LISTA DE SIGLAS E ABREVIATURAS

DR – Diário da república

LC – Lei do Cibercrime

CPP – Código de Processo Penal

CP – Código Penal

IP – *Internet protocol*

SMS – Serviço de mensagens curtas

IM – *Instant messaging*

BVerfG - *Bundesverfassungsgericht*

StPO – Código de Processo Penal Alemão

MP – Ministério público

OLG – *Oberlandsgericht* de Hamburgo

BGH – Tribunal Federal Alemão

Op. Cit. – *Opus citatum*

Ss - Seguintes

GG – Lei Fundamental da República Federal da Alemanha

CDFUE – Carta dos Direitos Fundamentais da União Europeia

ÍNDICE

<i>AGRADECIMENTOS</i>	1
<i>RESUMO E PALAVRAS-CHAVES</i>	2
<i>ABSTRACT</i>	4
<i>LISTA DE SIGLAS E ABREVIATURAS</i>	6
<i>ÍNDICE</i>	7
<i>1. INTRODUÇÃO</i>	10
<i>2. LEI DO CIBERCRIME, LEI N.º 109/2009, DE 15 DE SETEMBRO</i>	12
2.1. Enquadramento internacional	12
2.1.1. Convenção de Budapeste sobre o cibercrime	12
2.1.2. Decisão-Quadro nº. 2005/222/JAI, do Conselho, de 24 de fevereiro..	13
2.2. Enquadramento nacional	14
2.2.1. Lei do Cibercrime, enquanto lei extravagante	15
2.2.2. A dimensão processual da Lei do Cibercrime	17
<i>3. APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÕES DE NATUREZA SEMELHANTE</i>	20
3.1. Origem e definição de correio eletrónico	20
3.2. Definição de registos de comunicações de natureza semelhantes	22
3.3. Direitos fundamentais restringidos pela apreensão de correio eletrónico ..	22
3.3.1. Direito da inviolabilidade de correspondência e comunicações.....	24
3.3.2. Direito à autodeterminação informacional	26
3.3.3. Direito à reserva da intimidade da vida privada e familiar.....	27
3.3.4. Direito à palavra	28
3.4. Regime aplicável: articulação entre o artigo 179º do Código de Processo Penal e o artigo 17º da Lei do Cibercrime	29
3.4.1. A imperatividade do despacho judicial prévio	29

3.4.2. A figura do juiz, enquanto a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico	30
3.4.3. Acórdão do Tribunal Constitucional n.º 687/2021	34
3.4.4. (In)exigibilidade de punição com pena de prisão superior, no seu máximo, a 3 anos	36
3.4.5. A problemática da distinção entre correio eletrónico fechado/não lido e aberto/lido	38
4. <i>CONHECIMENTOS FORTUITOS</i>	41
4.1. Distinção entre conhecimentos de investigação e conhecimentos fortuitos	41
4.2. Considerações à luz das jurisprudências e das doutrinas alemã e portuguesa, anteriores à Lei n.º 48/2007, de 29 de agosto	42
4.2.1. Jurisprudência e doutrina alemãs	43
4.2.2. Jurisprudência e doutrina portuguesas	44
4.3. Valoração dos conhecimentos fortuitos, no âmbito das escutas telefónicas, à luz da Lei n.º 48/2007, de 29 de agosto	45
4.3.1. 1º Requisito: obtenção de conhecimentos fortuitos, a partir de escutas telefónicas válidas, no âmbito do primeiro processo	46
4.3.2. 2º Requisito: as provas obtidas, que constituem os conhecimentos fortuitos, reportam-se a um crime de catálogo	47
4.3.3. 3º Requisito: âmbito subjetivo considerado pelo artigo 187º, n.º 7 do CPP	48
4.3.4. 4º Requisito: a indispensabilidade da valoração dos conhecimentos fortuitos, para provar os factos reconduzíveis à verificação do tipo de ilícito	49
4.3.5. 5º Requisito: a prolação do despacho judicial a autorizar a transmissão dos conhecimentos fortuitos, para o segundo processo	50
4.4. Aproveitamento de correspondência eletrónica, no processo penal, já apreendida e valorada à ordem de outro processo	50
5. <i>CONCLUSÃO</i>	55
6. <i>JURISPRUDÊNCIA</i>	57

7. BIBLIOGRAFIA.....59

1. INTRODUÇÃO

Ao longo das últimas décadas do século XXI, o ambiente digital tem sido palco de um aumento claro de condutas cibercriminosas, nas mais variadíssimas frentes. Os agentes cibercriminosos aproveitam-se das vulnerabilidades de terceiros, que usufruem dos meios informáticos para fins legítimos¹.

De forma a reduzir a atividade criminosa, e consequentemente, proporcionar um aproveitamento legítimo dos meios informáticos na utilização diária, o legislador ordinário português publica a Lei do Cibercrime, igualmente intitulada por Lei n.º 109/2009, de 15 de setembro, em D.R. Esta resulta da combinação de diplomas internacionais, como se averiguará *infra*.

A questão crucial em torno do qual é realizado o estudo consiste em conhecer e compreender a possibilidade da valoração de mensagens de correio eletrónico, num processo diverso daquele, onde estas foram apreendidas e valoradas. A problemática tem chegado aos tribunais da relação. A lei portuguesa não estipula a possibilidade de valoração de conhecimentos fortuitos, no âmbito da apreensão² de mensagens de correio eletrónico, de forma clara e expressa. Todavia, esta temática encontra previsão no artigo 187º, n.º 7 e n.º 8 do CPP, relativamente às escutas telefónicas. A resolução desta problemática passará pelo paralelismo efetuado entre o regime aplicável, na apreensão de mensagens de correio eletrónico e nas escutas telefónicas, num primeiro momento. De seguida, a resolução passará pela análise, não só da possibilidade de valoração das mensagens apreendidas, num processo distinto daquele que lhe deu origem, bem como dos moldes em que tal sucederá. O ponto de partida do segundo passo consiste na compreensão dos requisitos impostos para a valoração dos conhecimentos fortuitos, no seio das escutas telefónicas.

A apreensão de mensagens de correio eletrónico consiste numa disposição processual consagrada no artigo 17º da LC, com remissão para o regime de apreensão de correspondência, previsto no CPP. Isto é, 179º e 252º do CPP. Visto que o legislador ordinário não dispensou o artigo 17º da LC, nos termos do artigo 11º do mesmo diploma, este meio processual poderá ser mobilizado em processos cujos crimes estejam estipulados

¹ VERDELHO, Pedro, “A nova lei do cibercrime”, *Scientia iuridica*, Tomo LVIII, n.º 320 (2009), página 717.

² O ato de apreender consiste em, ou tomar posse judicialmente, ou confiscar ou capturar mensagens de correio eletrónico. Veja-se, <https://www.infopedia.pt/dicionarios/lingua-portuguesa/Apreender>.

na LC, naqueles em que os crimes sejam cometidos por meio informático e naqueles relativos a crimes, em que seja necessário recolher prova em suporte informático. Portanto, este possui um âmbito de aplicação vasto.

Os conhecimentos fortuitos encontram-se estipulados no capítulo das escutas telefónicas, exclusivamente. Estas são um meio de obtenção de prova mais intrusivo nos direitos fundamentais, que o método anterior. O regime diferencia-se no seu âmbito de aplicação, por exemplo, uma vez que para estas, o legislador exige a verificação de um crime de catálogo, artigo 187º, n.º 1 e n.º 2 do CPP. O seu regime será mais exigente, o que se verificará na imposição de requisitos para a valoração dos conhecimentos fortuitos, igualmente.

2. LEI DO CIBERCRIME, LEI N.º 109/2009, DE 15 DE SETEMBRO

2.1. Enquadramento internacional

2.1.1. Convenção de Budapeste sobre o cibercrime

Com a finalidade de definir e punir os crimes informáticos, surge a Lei da Criminalidade Informática, a Lei n.º 109/91, de 17 de agosto, inspirada na Recomendação n.º R (89) 9 do Conselho da Europa, de 13 de setembro. Consta-se que ao longo das últimas décadas, tem-se verificado, não só o facilitismo no que ao acesso à informática concerne, como também uma evolução tecnológica e científica. Concomitantemente, a “realidade dos dias de hoje não é seguramente a mesma realidade à qual se destinava a Lei de 1991”³.

No final da última década do século XX, iniciaram-se os preparativos para aquela que haveria de se denominar por Convenção do Cibercrime⁴ ou Convenção de Budapeste. Após 4 anos de discussão, esta foi aprovada no dia 23 de novembro de 2001, em Budapeste. A convenção foi assinada por 3 dezenas de estados, englobando os membros do Conselho da Europa, EUA, Japão, Canadá e África do Sul, o que demonstra a sua “vocação universal”⁵. Em Portugal, a convenção em análise não foi aprovada imediatamente⁶.

Pedro Verdelho destaca vastos objetivos, de entre os quais se salienta a criminalização das condutas, a promoção de investigações criminais, a agilização da temática relativa à cooperação policial e judiciária, e para finalizar, a harmonização das legislações penais, num espírito de globalização entre nações⁷. “O limite de cada jurisdição nacional é decalque artificial, que transforma a realidade real num conceito virtual.”⁸.

A convenção é constituída por 4 capítulos. No artigo 1º, esta trata as definições de “Sistema informático” (alínea a)), “Dados informáticos” (alínea b)), “Prestador de serviços” (artigo c)) e “Dados de tráfego” (alínea d)). A convenção agrupa em capítulos, as matérias

³ VERDELHO, Pedro, “A nova Lei do Cibercrime”, op. cit., página 717.

⁴ Disponível em, <https://files.dre.pt/1s/2009/09/17900/0635406378.pdf>.

⁵ VERDELHO, Pedro, “A obtenção de prova no ambiente digital”, *Revista do Ministério Público*, n.º 99 (2004), página 125.

⁶ ASCENSÃO, J. de Oliveira, “O Cibercrime”, *Direito Penal Económico e Financeiro*, Coimbra Editora, 2012, página 310.

⁷ VERDELHO, Pedro, “A Convenção sobre Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa”, *Direito da Sociedade da Informação*, Vol. VI, Coimbra Editora, 2006, página 258.

⁸ VERDELHO, Pedro, “A obtenção de prova no ambiente digital”, op. cit., página 125.

relativas ao direito penal substantivo (artigos 2º a 13º), ao direito penal processual (artigos 14º a 22º), à cooperação judiciária e internacional (artigos 23º a 35º) e algumas disposições finais (artigos 36º a 48º).

A legislação portuguesa já previa as incriminações estipuladas na convenção. Quanto à vertente processual, surgem novas figuras, enquanto outras já possuíam previsão no CPP, sendo contextualizadas em ambiente digital. As inovações ressurgem no capítulo direcionado para a cooperação internacional. De acordo com a perspetiva avançada por Pedro Verdelho, a lei não é de todo revolucionária, uma vez que a recomendação que a alavancou, já tivera sido considerada com a entrada em vigor da Lei da Criminalidade Informática⁹.

2.1.2. Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro

A Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro de 2005 diz respeito a ataques contra sistemas de informações. A criminalidade organizada representava uma ameaça crescente aos sistemas informáticos, devido aos ataques terroristas constantes. Esta constatação toma uma dimensão mais expansiva, na medida em que os sistemas informáticos visados constituem as pedras basilares dos Estados-Membros. No contexto digital, o ambiente harmonioso é posto em causa. A decisão-quadro estipula um conjunto de definições no artigo 1º, a fim de garantir que estas constituíssem um elenco de designações comuns a todos os Estados-Membros. Este elenco é composto pelas denominações de “Sistema informático” (alínea a)), “Dados informáticos” (alínea b)), “Pessoa coletiva” (alínea c)) e “Não autorizado” (alínea d)). As sanções que venham a ser estabelecidas pelos Estados-Membros devem apresentar-se como efetivas, proporcionais e dissuasivas, para que o combate a estes ataques seja próspero. Para além da previsão relativa à responsabilidade das pessoas coletivas (artigo 8º), a decisão-quadro inclui 3 tipos de ilícitos, sendo estes o “Acesso ilegal aos sistemas de informação” (artigo 2º), a “Interferência ilegal no sistema” (artigo 3º) e “Interferência ilegal nos dados” (artigo 4º). A decisão-quadro ambiciona que haja respeito pelos direitos fundamentais e pelos princípios reconhecidos pelo artigo 6º do

⁹ VERDELHO, Pedro, “A convenção sobre o cibercrime do conselho da europa – repercussões na lei portuguesa”, *Direito da Sociedade da Informação*, op. cit., páginas 258 e 259.

Tratado da União Europeia e a Carta dos Direitos Fundamentais da União Europeia¹⁰ (CDFUE).

O objetivo da decisão-quadro consiste em “vencer nominalisticamente as resistências quanto a uma competência da Comunidade Europeia em matéria penal.”¹¹ A ambição do diploma caracteriza-se pela aproximação do direito penal entre Estados-Membros, no que à matéria sobre ataques contra sistemas informáticos concerne.

Nos termos do artigo 12º da decisão-quadro, “os Estados-Membros devem tomar as medidas necessárias para dar cumprimento às disposições da presente decisão-quadro até 16 de março de 2007”. Em Portugal, a decisão-quadro foi transposta através da Lei do Cibercrime, em 2009, tendo apresentado um período de atraso de 2 anos.

A Diretiva 2013/40/EU do Parlamento Europeu e do Conselho, de 12 de agosto de 2013 veio substituir a Decisão-Quadro 2005/222/JAI. A substituição (artigo 15º da diretiva) consiste na implementação de alterações “numerosas e substanciais”, em relação à decisão-quadro (34). Desta forma, a diretiva estabelece que a substituição deveria ser integral para os Estados-Membros que a adotassem. A finalidade da diretiva prende-se com a aproximação do direito penal dos Estados-Membros, relativamente a ataques contra os sistemas de informação (1), o que se assemelha ao objetivo traçado pela decisão-quadro anterior¹².

Ao longo de doze anos de vigência, a Lei do Cibercrime não sofreu quaisquer alterações legislativas.

2.2. Enquadramento nacional

A LC ou Lei n.º 109/2009, de 15 de setembro¹³ resulta da combinação de duas fontes de direito europeu, isto é, da transposição da Decisão-Quadro 2005/222/JAI, do Conselho, de 24 de fevereiro e da adaptação do direito interno, com a Convenção do Cibercrime. A LC é constituída por 5 capítulos, intitulados por “Objeto e definições”,

¹⁰ Acessível em, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32005F0222&from=PT>.

¹¹ ASCENSÃO, J. de Oliveira, “O Cibercrime”, op. cit., página 311.

¹² Disponível em, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=PT>

¹³ In, <https://dre.pt/dre/detalhe/lei/109-2009-489693>.

“Disposições penais e materiais”, “Disposições processuais”, “Cooperação internacional” e “Disposições finais e transitórias”, respetivamente. No capítulo III, relativo às disposições processuais, reconhece-se a existência de meios processuais que correspondem a figuras novas, enquanto outras se reconduzem a figuras processuais já existentes no CPP, porém adaptadas em contexto digital. O primeiro conjunto é composto pela “Preservação expedita de dados” (artigo 12º), “Revelação expedita de dados de tráfego” (artigo 13º) e “Injunção para a apresentação ou concessão do acesso a dados” (artigo 14º). O segundo é constituído pela “Pesquisa de dados informáticos” (artigo 15º), “Apreensão de dados informáticos” (artigo 16º), “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante” (artigo 17º), “Interseção de comunicações” (artigo 18º) e “Ações encobertas” (artigo 19º).

A entrada em vigor da LC culmina na revogação da Lei da Criminalidade Informática, também qualificada por Lei n.º 109/91, de 17 de agosto (artigo 30º da LC).

Visto que o estudo incide sobre a apreensão de mensagens de correio eletrónico e registos de comunicações de natureza semelhantes, debruçar-me-ei sobre a sua origem. Contrariamente ao que seria expectável, esta não resulta das fontes de direito europeu analisadas *supra*, considerando que em ambas não se verifica quaisquer disposições direcionadas para este meio de obtenção de prova, especificadamente. Este nasce a partir da Proposta de lei n.º 289/X/4ª, nomeadamente do seu artigo 19º. O legislador pretendeu adaptar os regimes das buscas e apreensões, previstos no CPP, para o ambiente digital¹⁴. Este “propôs-se adaptar este regime, não aplicá-los integral e acriticamente”¹⁵.

2.2.1. Lei do Cibercrime, enquanto lei extravagante

A doutrina tem debatido a ausência da inserção sistemática das normas da LC, no CPP, tendo o legislador ordinário optado por a consagrar enquanto lei extravagante, em 2009. Paulo Dá Mesquita¹⁶, João Conde Correia e Sónia Fidalgo afirmam que as normas

¹⁴

Disponível

em,

<https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalleIniciativa.aspx?BID=34566>.

¹⁵ CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009”, de 15.IX”, *Revista do Ministério Público*, n.º 153 (2018), página 170.

¹⁶ Dá Mesquita sugere que, caso a inserção das normas da LC, no CPP, tivesse tomado lugar, estas encontrar-se-iam englobadas no capítulo III, relativo às disposições processuais, constaria do capítulo V, direcionado para a prova eletrónica, no Título III, no qual se aborda os meios de obtenção de prova, no Livro

relativas à prova digital, nomeadamente a LC, deveriam compor o conjunto das normas do CPP, perspetiva que subscrevo. A não inclusão das normas da LC demonstra espírito de arrumação e uma redução aparente do número de revisões a que o código estaria sujeito. Automaticamente, a introdução da LC implicaria uma revisão, bem como quaisquer alterações a estas normas. Aspirava-se que a “separação de águas” proporcionasse a estabilidade jurídica, o que não sucedera. Contemporaneamente, o CPP é constantemente revisto, ano após ano, contrariamente ao que sucede com a LC. Desde 2009, esta nunca sofrera quaisquer alterações, tendo se desenvolvido, em 2021, pela primeira vez, uma proposta de alteração do artigo 17º da mesma, tendo esta sido declarada inconstitucional pelo TC¹⁷.

Dá Mesquita salienta que a dispersão das normas em lei extravagante tornar-se-ia inconveniente, destacando a importância da inserção destas normas no CPP, face ao crescente número de condutas criminosas realizadas em contexto informático¹⁸.

João Conde Correia reconhece que a dissipação das leis entre o CPP e a LC potencia a insegurança jurídica e, por isso, a crise na justiça, devido à instabilidade, complexidade e confusão legislativas¹⁹. Este autor refere que esta circunstância traduz uma “descodificação sistemática regressiva”²⁰. O legislador privilegiou o particular, em detrimento do global. Pela sua importância, pelos interesses envolvidos, pela frequência em que as normas são interpretadas e as consequências que daí advêm, demonstra-se que a sua qualificação enquanto lei extravagante é errónea. A inserção das normas no CPP reduziria a complexidade instalada, uma vez que o interprete não apresentaria quaisquer dificuldades em selecionar a lei a aplicar. “Leges non sunt multiplicandae sine necessitate”²¹. O desenvolvimento de um sistema tendencialmente unitário da prova digital penal, capaz de salvaguardar a proteção dos direitos fundamentais, seria despoletado aos olhos deste autor²².

Sónia Fidalgo destaca que estas regras se aplicam aos processos cujos crimes, ou se encontrem previstos na LC, ou sejam praticados através de meio informático, ou nos quais

III do CPP, cujo tema é prova. MESQUITA, P. Dá, “ Prolegómenos sobre prova eletrónica e intercepção de telecomunicações no Direito Processual Penal Português – o Código e a Lei do Cibercrime”, *Processo Penal, Prova e Sistema Judiciário*, Wolters Kluwer / Coimbra Editora, 2010, página 101.

¹⁷ Veja-se, <https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html>.

¹⁸ MESQUITA, P. Dá, op. cit., página 101.

¹⁹ CORREIA, J. Conde, “Prova Digital: as leis que temos a lei que devíamos ter”, *Revista do Ministério Público*, n.º 139 (2014), página 53.

²⁰ *Idem*, página 54.

²¹ *Idem*, página 55.

²² *Idem*, página 56.

seja essencial recolher prova, presente em sistema informático. Portanto, estas regras dizem respeito a processos, cujos crimes estejam estipulados no CP. Realça ainda que as dificuldades de harmonização com as normas do CPP²³ (artigos 179º e 189º) e as leis extravagantes seriam colmatadas, eventualmente (Lei nº 32/2008)²⁴.

Acredito que o legislador ordinário não se satisfaria com a simples introdução das normas da LC. Por iniciativa própria, resolveria as contradições existentes entre estas e outras normas existentes no CPP e outras leis extravagantes, reajustando-as.

2.2.2. A dimensão processual da Lei do Cibercrime

2.2.2.1. Âmbito de aplicação das disposições processuais, artigo 11º da Lei do Cibercrime

O artigo 11º da LC consagra o âmbito de aplicação das disposições processuais. De acordo com o mesmo, os meios de obtenção de prova previstos neste capítulo aplicar-se-ão a processos relativos a crimes, previstos na LC (alínea a)), que sejam cometidos através de meios informáticos (alínea b)) e quaisquer outros, em que seja necessário obter prova em suporte eletrónico (alínea c)), em regra.

Todavia, o legislador ordinário estabeleceu a interseção de comunicações e ações encobertas, estipuladas nos artigos 18º e 19º, respetivamente, enquanto exceções ao âmbito de aplicação apresentado. Estes meios processuais consagram os seus catálogos de crimes, o que se justifica pelo caráter intrusivo em relação aos direitos fundamentais dos mesmos. Esta é uma das várias demonstrações da procura pela concordância prática²⁵ entre as finalidades processuais, uma vez que estes meios de obtenção de prova não são mobilizados sem mais.

O conceito de criminalidade informática não tem presença expressa na legislação, ou qualquer densificação na doutrina e jurisprudência. Pedro Verdelho salienta a distinção entre criminalidade informática em sentido amplo e a criminalidade em sentido estrito. A primeira caracteriza-se como a tipologia que abrange as condutas criminosas efetuadas

²³ *Infra*, evidencia-se várias dificuldades, que emergem da tentativa de compatibilização entre as normas da LC e do CPP. Veja-se, as páginas 18 e ss e 29 e ss.

²⁴ FIDALGO, Sónia, “Apreensão de correio eletrónico e utilização noutra processo das mensagens apreendidas”, *Revista Portuguesa de Ciência Criminal*, n.º 1 (2019), página 61.

²⁵ Breve referência, *infra* nas páginas 22 e 23.

através da informática, sendo esta um dos meios que o agente poderia mobilizar para consumir o tipo de ilícito. A informática não é parte integrante do mesmo. A segunda pressupõe que a informática seja o meio através do qual a atividade criminosa se concretiza. A informática constitui o tipo de ilícito²⁶. Analisando o artigo 11º, n.º 1 da LC e a distinção avançada pelo autor, rapidamente se compreende a correspondência entre ambos. As alíneas a) identificam a criminalidade em sentido estrito, enquanto a alínea b) se direciona para a criminalidade em sentido amplo.

2.2.2.2. A problemática da extensão legal promovida pelo artigo 189º do Código de Processo Penal

No que ao seu enquadramento legislativo concerne, o artigo 189º do CPP encontra-se no capítulo IV (“Das escutas telefónicas”), título III (“Meios de obtenção de prova), livro III (“Prova”). Em 1998, o legislador ordinário estendeu o regime a aplicar às escutas telefónicas, às “conversações ou comunicações transmitidas por qualquer meio técnico diferente de telefone, designadamente, o correio eletrónico ou outras formas de transmissão de dados por via telemática, bem como à interseção das comunicações entre presentes”²⁷, consagrando-o no artigo 190º do CPP. Com a revisão de 2007, o mesmo não só aditou a expressão “mesmo que se encontrem guardados em suporte digital”, referindo-se às comunicações efetuadas por correio eletrónico, como também o artigo específico passou a ser o artigo 189º do CPP, sem prejuízo da manutenção do restante corpo da norma²⁸.

A controvérsia doutrinal e jurisprudencial²⁹ origina-se com entrada em vigor da LC, em 2009. Esta possui um regime díspar para a apreensão de correspondência eletrónica e registos de comunicações de natureza semelhantes (artigo 17º), sendo que este remete para as normas relativas à apreensão de correspondência do CPP (artigo 179º), contrariamente ao

²⁶ VENÂNCIO, P. Dias, *Lei do Cibercrime Anotada e Comentada*, Coimbra Editora, 2011, páginas 16 e 17.

²⁷ Disponível em https://www.pgdlisboa.pt/leis/lei_print_articulado.php?tabela=lei_velhas&artigo_id=&nid=199&nversao=9&tabela=lei_velhas.

²⁸Ver, https://www.pgdlisboa.pt/leis/lei_print_articulado.php?tabela=lei_velhas&artigo_id=&nid=199&nversao=18&tabela=lei_velhas.

²⁹ No acórdão do TC, n.º 687/2021, quando questionado acerca da possível inconstitucionalidade da proposta de alteração ao artigo 17º da LC, este menciona que o regime aplicável consta deste artigo, bem como do artigo 179º do CPP. In, <https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html>.

que sucede no artigo 189º, que direciona para os artigos 187º e 188º do CPP. Em momento algum, a LC assume de forma clara e expressa, a alteração do artigo 189º, n.º 1, revogando-o parcialmente³⁰. Face ao exposto, a revogação, na parte que concerne ao correio eletrônico, será o desejável. O legislador, apesar das várias possibilidades concedidas, através de constantes revisões para o efetuar, a revogação parcial nunca se promoveu, sendo tal tarefa o desejável, a fim de garantir a estabilidade jurídica.

Benjamin Silva Rodrigues reconhece que a entrada em vigor da LC submeteu o correio eletrônico a um regime dual, contradizendo-se. Ao menosprezar a diferenças inerentes às respetivas regulamentações, a infelicidade é o sentimento vivenciado pela atitude do legislador³¹. Tiago Milheiro estranhou o aditamento da expressão “mesmo que se encontrem guardadas em suporte digital”. Esta expressão aponta para as mensagens de correio eletrônico que se encontram armazenadas em suporte digital, pelo que as respetivas comunicações não se encontram a decorrer em tempo real. Realça que o artigo 17º da LC é aquele que deve ser mobilizado nestas circunstâncias. Este caracteriza-se pela sua “autonomia própria e distinta da vertida nos artigos 187º e 188º do CPP”. Consequentemente, este autor defende a revogação do segmento mencionado³².

Pessoalmente, aproximo-me das posições previamente mencionadas. A LC consiste numa lei extravagante direcionada para o ambiente digital, de forma a colmatar o crescente aumento do número de condutas criminosas neste meio. Invocando à colação, o princípio segundo o qual, a lei especial derroga a lei geral (“*Lex specialis derogat legi generali*”), e sendo a LC uma lei especial, não se compreende as razões pelas quais, o legislador não procedeu à revogação parcial e formal do artigo 189º do CPP, relativamente ao correio eletrônico³³.

De olhos postos nos regimes diversificados dos artigos 17º da LC e 189º do CPP, há que relembrar que o primeiro remete para o regime relativo à apreensão de correspondência do artigo 179º do CPP, enquanto o segundo assume a implementação do regime relativo às escutas telefónicas (artigos 187º e 188º do CPP). Analisando a apreensão

³⁰ MESQUITA, P. Dá, op. cit., páginas 102, 105, (notas 43) e 117.

³¹ RODRIGUES, B. Silva, *Da Prova Penal, Bruscamente... A(s) face(s) ocultas(s) dos métodos ocultos de investigação criminal*, Tomo II, Rei dos Livros, 2010, páginas 453 e 454.

³² MILHEIRO, T. Caiado, “Artigo 189º”, *Comentário Judiciário do Código de Processo Penal*, Tomo II, 2ª Edição, Almedina, 2020, página 813.

³³ CORREIA, J. Conde, “Prova Digital: as leis que temos e a lei que devíamos ter”, op. cit., página 36.

da correspondência eletrônica e as escutas telefônicas individualmente, rapidamente se entende que o segundo meio de obtenção de prova é mais lesivo, no que à restrição de direitos fundamentais diz respeito, sendo que este consiste numa “investigação oculta”³⁴. Consequentemente, o regime aplicável será mais exigente (catálogo de crimes mais restrito, por exemplo), uma vez que o legislador ordinário procura, incessantemente, pela concordância prática entre as finalidades processuais³⁵, nomeadamente a descoberta da verdade material e a realização da justiça e a defesa dos direitos fundamentais do arguido e de terceiros, perante o Estado. O regime é pensado para cada meio de obtenção de prova, já que cada um tem as suas características próprias, devendo este ser proporcional ao mesmo, (artigo 18º, n.º 2 da CRP). Sabendo que o regime previsto nos artigos 187º e 188º é mais gravoso e que se encontra em vigor a LC, na qual se prevê um regime próprio (artigo 17º), qual será o sentido de se prever a extensão pelo artigo 189º, e consequente aplicação, aquando da apreensão de correspondência eletrónica?

No artigo 189º, n.º 1 do CPP, a estipulação da extensão do regime das escutas telefónicas, às mensagens de correio eletrónico guardadas em suporte digital é suficiente para que o interprete recorra aos artigos 187º, 188º do CPP, por lapso, aquando da desconsideração total da existência do artigo 17º da LC.

3. APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÕES DE NATUREZA SEMELHANTE

3.1. Origem e definição de correio eletrónico

Na década dos anos 60, surgiu o primeiro computador. Contudo, o grande impulso para a utilização da correspondência eletrónica consistiu na criação do programador informático norte americano, denominado por Ray Tomlinson. Este era capaz de enviar mensagens entre dois computadores distantes, unicamente ligados por uma rede informática.

³⁴ Costa Andrade, “Métodos ocultos de investigação (Pladoyer para uma teoria geral)”, página 532, apud ANTUNES, M. João, *Direito Processual Penal*, 2ª Edição, Reimpressão, Almedina, 2019, página 123.

³⁵ DIAS, J. Figueiredo, “O Novo Código de Processo Penal”, *Textos Jurídicos – I*, Ministério da Justiça, 1987, página 13.

Posteriormente, criaram-se protocolos de transmissão e receção de mensagens de servidores de correio eletrónico, tais como o SMTP (*simple mail transfer protocol*) e POP (*post office protocol*), tendo estes permitido o acesso às caixas de correspondência em dispositivos móveis³⁶.

O conceito de correio eletrónico “é algo que pode não ser claro.”³⁷. Apesar do silêncio legislativo, a doutrina tem vindo a apresentar diversas definições. De acordo com a perspetiva de Carlos Casabona, as mensagens de correio eletrónico são “uma modalidade de comunicação, no geral de carácter pessoal, que incorpora texto, voz, som e imagem e que se serve das redes informáticas como tecnologia de transmissão e dos sistemas informáticos (computadores e o software ou sistema lógico correspondente) como instrumentos de emissão e receção entre os dois ou mais comunicantes e nesse caso de armazenamento de mensagens.”³⁸. Rui Cardoso acrescenta que as mensagens são constituídas pelo conteúdo, dados de tráfego, que se encontram nos cabeçalhos, quando transmitidas entre destinatário e remetente, através da Internet. Não obstante as diferenças técnicas, comparativamente ao meio anterior, a transmissão efetuada por meio de internets encontra-se tutelada pelo âmbito de aplicação do artigo 17º³⁹. Nas palavras de Armando Dias Ramos, correio eletrónico consiste num “programa informático que permite a comunicação instantânea, de modo diferido, entre quem a envia e quem a recebe, através de redes de informação e comunicação, independentemente, do local em que estes se encontrem, sem a necessidade deste se encontrar instalado no computador.”. Concomitantemente, o autor destaca características, das quais se destaca o carácter eletrónico, assíncrono, ubíquo, digital e informacional⁴⁰.

Tem-se convocado a definição estipulada no artigo 2º, alínea f), da Diretiva 202/58/CE, do Parlamento Europeu e do Conselho, em virtude da vinculatividade ao direito da união europeia. O correio eletrónico designa-se por “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

³⁶ RAMOS, A. Dias, *A prova digital em processo penal: o correio eletrónico*, 2ª Edição, Chiado Editora, 2017, páginas 27 e 28.

³⁷ CARDOSO Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei nº. 109/2009, de 15.IX”, op. cit., página 180.

³⁸ CASABONA, C. M. Romeo, “La protección penal de los mensajes de correo electrónico Y de otras comunicaciones de carácter personal a través de la red”, páginas 48 e 49. Disponível em <https://www.metodista.br/revistas/revistas-izabela/index.php/dih/article/view/135>.

³⁹ CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei nº. 109/2009, de 15.IX, op. cit., página 181.

⁴⁰ RAMOS, A. Dias, op. cit., páginas 31 e 32.

recolher.”⁴¹. Todavia, o legislador português não teve a preocupação em considerar esta definição, aquando da transposição da diretiva para o direito interno, nomeadamente, nos artigos 2º e 17º da LC, relativos às definições e à apreensão de correspondência eletrónica e de registos de comunicações de natureza semelhante, respetivamente⁴².

3.2. Definição de registos de comunicações de natureza semelhantes

Os registos de comunicações de natureza semelhante são efetuados, ora por meio do telefone, ora pela Internet, através da utilização de Protocolos TCP (*transmission control protocol*) / IP (*internet protocol*), que implicará a entrega de um IP *Adress*. Relativamente, ao primeiro método, destacaram-se as SMS (serviços de mensagens curtas), EMS (serviço de mensagens desenvolvido) e MMS (serviço de mensagens multimédia). O emprego da Internet, enquanto meio de transmissão, engloba as comunicações por IM⁴³, tais como, *Instant Messenger* e *Chat* ou *Chatrooms*^{44 45}.

Na eventualidade de a investigação versar sobre a apreensão de registos de comunicações de natureza semelhante, o regime aplicável corresponde ao estipulado para a apreensão de correio eletrónico, de acordo com o estipulado pelo artigo 17º da LC.

3.3. Direitos fundamentais restringidos pela apreensão de correio eletrónico

O processo penal português é composto por três finalidades: o restabelecimento da paz jurídica comunitária e do arguido, a realização da justiça e a descoberta da verdade material e a proteção dos direitos fundamentais do arguido e de terceiros, perante o Estado.

⁴¹ Consultar em, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT>.

⁴² RAMOS, A. Dias, op. cit., página 29.

⁴³ IM ou programas de mensagens instantâneas pressupõem o envio e a receção de textos, áudios, ficheiros e a realização de videoconferências em tempo real. O respetivo envio e receção é condição suficiente para que as mensagens sejam armazenadas e suscetíveis de apreensão. CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX”, op. cit., página 183.

⁴⁴ Os *chatrooms* designam os locais virtuais, públicos ou privados, nos quais duas ou mais pessoas se encontram para partilhar mensagens ou ficheiros, com finalidades lícitas e ilícitas. Estes podem determinar uma forma para o ocultar, sendo que poderão ser guardados por qualquer interveniente. CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/209, de 15. IX”, op. cit., página 183.

⁴⁵ CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX”, op. cit., página 181 a 183.

Apesar de o desejável consistir no estabelecimento de um equilíbrio entre as várias finalidades, estas conflituem entre si. Por isso, o processo penal português possui um caráter irremediavelmente antinómico e antitético”⁴⁶.

De forma a promover e a salvaguardar o máximo conteúdo possível de cada finalidade, deve procurar-se a concordância prática entre as mesmas. A concessão de uma relevância predominante a uma finalidade caracteriza-se como sendo uma “solução antidemocrática e totalitária”, na perspectiva de Figueiredo Dias. Tudo isto, não obstante o limite inultrapassável em qualquer circunstância, denominado por dignidade da pessoa humana,⁴⁷ (artigo 1º da CRP).

A apreensão de mensagens de correio eletrónico e de registos de comunicações de natureza semelhante, enquanto meio de obtenção de prova, impulsiona a descoberta da verdade material e a realização da justiça. Contudo, o caráter lesivo deste meio é inegável, uma vez que instigará o acesso, na sua plenitude, a vastas informações pessoais, possibilitando a construção da vida do indivíduo, cujas mensagens tenham sido apreendidas. Portanto, colocar-se-á em questão determinados direitos fundamentais. De forma a acautelar a concordância prática entre as finalidades em conflito, o legislador ordinário estipulou a possibilidade de apreensão, desde que verificados os pressupostos para tal, sendo estes analisados *infra*⁴⁸.

Devido à mobilização deste meio de obtenção de prova e à conseqüente manifestação negativa no proveito absoluto dos direitos, liberdades e garantias dos cidadãos, passarei a explicitar os direitos restringidos⁴⁹.

⁴⁶ DIAS, J. Figueiredo, “O Novo Código de Processo Penal”, op. cit., página 13.

⁴⁷ *Ibidem*.

⁴⁸ Veja-se, páginas 29 e ss.

⁴⁹ Nos variadíssimos diplomas, o direito da união europeia consagra a estipulação dos direitos apresentados *infra*. Destaca-se os artigos 7º e 8º da CDFUE, nos quais se prevê que “Todas as pessoas têm o direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.” e “Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.”, respetivamente. Visualizar em, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. O artigo 8º da Convenção Europeia para a proteção dos Direitos do Homem e das Liberdades Fundamentais transmite o exato sentido exposto no artigo 7º da CDFUE. Disponível em https://www.echr.coe.int/documents/convention_por.pdf.

3.3.1. Direito da inviolabilidade de correspondência e comunicações

O direito da inviolabilidade de correspondência e/ou de comunicações privadas concretiza-se no artigo 34º, n.º 1 da CRP, segundo o qual, “O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis”, reforçando-o no n.º 4, no qual “É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação”. Para além de quaisquer espécies de correspondência (cartas, postais, encomendas), o âmbito de aplicação deste artigo abrange as telecomunicações (telefone e telefax),⁵⁰ igualmente. O correio eletrónico goza da tutela conferida pelo artigo 34º da CRP, visto que este direito engloba as “correspondências mantidas por via das telecomunicações”⁵¹.

Este direito visa proteger bens jurídicos, como a dignidade da pessoa humana, o desenvolvimento da personalidade, a garantia da liberdade individual, autodeterminação existência e a garantia da privacidade, (artigo 26º da CRP)⁵². O legislador constitucional prevê que a ingerência poderá ser permitida excecionalmente, nos casos previstos na lei processual criminal, o que demonstra a procura incessante pela concordância prática. Dado que a ingerência é autorizada em circunstâncias restritas, torna-se imperioso uma apreciação drástica, de acordo com o princípio da proporcionalidade em sentido amplo, nos termos

⁵⁰ Em 1995, o termo “telecomunicação” veio substituir o conceito comunicação telefónica ou telegráfica, implementada em 1982. Este conceito apresenta um âmbito de aplicação indefinido, nas vastas áreas jurídicas. Não obstante a sua previsão no artigo 34º da CRP, este termo desapareceu de diversas leis. Nos termos do artigo 2º, n.º 1 da Lei n.º 91/97, de 1 de agosto, estipulou-se que “telecomunicação” consistiria na “transmissão, receção ou emissão de sinais, representando símbolos, escrita, imagens, sons ou informações de qualquer natureza por fios, por sistemas ópticos, por meios radioelétricos e por outros meios eletromagnéticos.” No seguimento da revogação desta lei, pela Lei das Comunicações Eletrónicas (Lei n.º 5/2004, de 10 de fevereiro), o termo “telecomunicação” desvanece da lei extra-penal. Todavia, a lei que entrou em vigor, através da consagração de definições de “rede de comunicação eletrónica” e “serviço de comunicação eletrónica”, instiga a elaboração da definição em análise, ainda que indiretamente. Para além da ausência desta definição na LC, a Lei n.º 32/2008, de 11 de julho, volta a definir “comunicação eletrónica”. Citando Costa Andrade, de acordo com a perspetiva generalizada, “telecomunicações” engloba “todos os procedimentos técnicos de transmissão incorpórea (contraposta à transmissão postal) à distância de qualquer espécie de informação ou notícias dirigidas a um destinatário individualizado”, independentemente, do sistema tecnológico, das formas de expressão e do seu conteúdo. A relação triádica pressupõe-se neste âmbito, sendo composta pelo emitente, pelo destinatário e pelo mediador. Realça-se que a tutela da incriminação exclui as telecomunicações públicas, de massa ou difusão, focando-se nas telecomunicações privadas ou endereçadas, exclusivamente. ANDRADE, M. Costa, “Anotação ao Artigo 194º”, *Comentário Conimbricense do Código Penal, Parte Especial*, Tomo I, 2ª Edição, Coimbra Editora, 2012, páginas 1093 a 1095.

⁵¹ CANOTILHO, J. J. Gomes/MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Vol. I, 4ª Edição Revista, Coimbra Editora, 2007, página 544.

⁵² *Idem*, página 539.

definidos pelo artigo 18º, nº2 da CRP⁵³ (“A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.”).⁵⁴

Conforme Costa Andrade, a tutela conferida através da previsão constitucional do artigo 34º da CRP encontra-se dependente do processamento da comunicação, estando este, sob o domínio da empresa fornecedora do serviço comunicacional. A proteção é atribuída até ao momento em que a comunicação entra na esfera do domínio do destinatário⁵⁵ (quando a mensagem se encontrar recebida e lida), sendo este o exato instante, em que termina o processo de comunicação⁵⁶. O conteúdo e as circunstâncias envolventes do mesmo abandonam a “específica situação de perigo”, e portanto, a circunstância que os reconduziria à carência de tutela, pelo artigo 34º da CRP. Clarifica que os indivíduos têm ao seu dispor meios de tutela, dos quais a instalação de meios de segurança e a destruição dos dados informáticos são exemplificativos, de forma a garantir a tutela retirada^{57 58}. Na perspetiva do

⁵³ No que à componente substancial diz respeito, o artigo 18º, n.º 2 e n.º 3 da CRP assemelha-se ao artigo 52º, n.º 1 da CDFUE, uma vez que neste, para além da restrição dos direitos, liberdades e garantias se encontrar estipulada no respetivo diploma internacional, a restrição dos mesmos deverá respeitar o seu conteúdo essencial. De olhos colocados no princípio da proporcionalidade em sentido amplo, as restrições permitidas limitar-se-ão, não só àquelas que sejam necessárias, como também às que correspondem às finalidades delineadas pela União ou à proteção dos direitos, liberdades e garantias.

⁵⁴ CANOTILHO, J. J. Gomes/MOREIRA, Vital, op. cit., página 543.

⁵⁵ Na perspetiva do BVerfG, o segredo das comunicações encontra-se estipulado no artigo 10º GG. Este é o garante do direito ao livre desenvolvimento da personalidade e, conseqüentemente, do princípio da dignidade da pessoa humana. O valor constitucional deste direito advém da proteção da confiança concedida, no momento da comunicação, quando esta é estabelecida entre o remetente e o destinatário, que se encontram espacialmente distantes. Neste instante, a transmissão é assegurada por terceiros, o que a caracteriza como sendo vulnerável à intervenção destes. Por conseguinte, os intervenientes principais encontram-se impossibilitados de assegurar a confidencialidade da comunicação. Devido à ausência de privacidade, a tutela atribuída consiste numa compensação, a fim de proteger os detalhes da comunicação, uma vez que estes possuem caráter declaratório. Caso contrário, a tutela seria escassa. Esta conceção finaliza assim que os dados atinjam a esfera do domínio do destinatário, o que fora potencializado pela semelhança atribuída entre os dados já recebidos e os produzidos pelo próprio. A receção pelo destinatário determina o momento a partir do qual este obtém o controlo dos dados, pelo que é capaz de impedir, não só o acesso a estes por terceiros, como também a manutenção ou eliminação dos mesmos. BVerfG, 2 BVR 2099/04 de 02/03/2006 *apud* RAMOS, Vânia, “Âmbito e Extensão do Segredo das Telecomunicações”, *Revista do Ministério Público*, n.º 11 (2007), páginas 147 e 148.

⁵⁶ ANDRADE, M. Costa, “Bruscamente no Verão Passado”, *A reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra Editora, 2009, página 159.

⁵⁷ *Idem*, página 158.

⁵⁸ Neste sentido, NUNES, D. Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018, página 147.

autor, este entendimento suscitará repercussões relativamente ao regime a aplicar, consoante estejam em análise, mensagens de correio eletrónico abertas ou fechadas⁵⁹.

Face à perspectiva exposta pelo autor, questiono como é que será exequível determinar o momento do término da tutela conferida pelo artigo 34º da CRP, com precisão, uma vez que atualmente enfrentamos dificuldades em demarcar o instante, a partir do qual se abre ou lê a mensagem de correio eletrónico⁶⁰. Acrescento que mesmo que a mensagem se apresente como aberta/lida, no sistema informático, o conteúdo da mesma permanece, contendo informações e dados pessoais. Estas carecem da tutela conferida pelo artigo 34º, n.º 1 e n.º 4 da CRP, uma vez que poderão ser sujeitas a apreensões, por exemplo.

3.3.2. Direito à autodeterminação informacional

O artigo 35º da CRP estipula o direito à autodeterminação informacional⁶¹, conferindo proteção, aquando do tratamento de dados pessoais informáticos aos cidadãos. A relevância atribuída à respetiva proteção, justifica-se pelo possível tratamento e mobilização abusiva de dados pessoais informáticos, o que se potenciou pelo desenvolvimento e aproveitamento dos meios informatizados⁶².

A densificação do direito à autodeterminação informacional resulta da conjugação do n.º 1 (“Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito (...), e o direito de conhecer a finalidade a que se destinam”), com o n.º 3 (“A informática não pode ser utilizada para tratamento de dados” pessoais), com o n.º 4 (“É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei”) e com o n.º 5 (“É proibida a atribuição de um número nacional único aos cidadãos”). O artigo 35º da CRP propicia que “cada pessoa tem o direito de controlar a informação disponível a

⁵⁹ Veja-se as páginas 38 e ss.

⁶⁰ Análise das dificuldades inerentes infra, páginas 38 e ss.

⁶¹ Na perspectiva do BVerfG, os dados armazenados pelo destinatário carecem de tutela constitucional, sendo fornecida pelo direito à autodeterminação informacional, estipulado no artigo 2º, n.º 1, conjugado com o artigo 1º, n.º 1 e 13º, n.º 1 GG. O tribunal designa-o como “a proteção do indivíduo contra a produção, armazenamento, utilização e divulgação dos dados pessoais, sendo condição, no presente, do livre desenvolvimento da personalidade”. Este argumenta que este direito possui uma função complementar à proteção conferida pelo segredo das comunicações. BVerfG, 2 BvR 2099/04 de 02/03/2006 *apud* RAMOS, Vânia, op. cit., páginas 149 e 150.

⁶² NEVES, R. Castanheira, *As ingerências nas comunicações eletrónicas em processo penal, Natureza e respectivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*, Coimbra Editora, 2011, páginas 57 e 58.

seu respeito, impedindo-se que a pessoa se transforme em um simples objeto de informações”⁶³.

Catarina Sarmiento e Castro considera que o direito à autodeterminação informacional se caracteriza como direito fundamental, sendo constituído pelo conteúdo que lhe é próprio. Apesar de se configurar como um direito garantístico do direito à reserva da intimidade da vida privada e familiar, este afigura-se como um direito de personalidade, que despoletará, não só o controlo sobre a utilização de informações pessoais, como também a proteção a conferir a estas, que se encontrem sujeitas a agressões abusivas. Numa vertente subjetiva, os titulares deste direito gozam de posições jurídicas, que lhes concederá segurança face às utilizações indevidas de dados pessoais pelo Estado. Por outro lado, a perspetiva objetiva promove a proteção destes dados através da tomada de providências pelo Estado, em relação a agressões por via de terceiros⁶⁴.

3.3.3. Direito à reserva da intimidade da vida privada e familiar

Relativamente ao direito à privacidade, sob influência da doutrina alemã, a doutrina portuguesa recorreu à Teoria das Três Esferas, composta pela esfera íntima (sentimentos, sexualidade e saúde), pela esfera privada (matérias relacionadas com a história do cidadão e o contexto social no qual se insere) e a esfera pessoal (abrange a vida pública e em comunidade)⁶⁵.

Vital Moreira e Gomes Canotilho, em anotação ao artigo 26º da CRP, para além de reconhecerem o direito à reserva da intimidade da vida privada e familiar, sustentam que se verifica uma dualidade entre o direito da impossibilidade de acesso a informações pessoais por terceiros, e o direito da não divulgação de informações pertencentes a terceiros. Estes autores desconsideram a distinção entre esferas, enaltecendo que o critério deveria partir dos conceitos de “privacidade” e “dignidade humana” (artigo 26º, n.º 1 e n.º 2 da CRP), com a finalidade de definir “o conceito de esfera privada de cada pessoa, culturalmente adequado

⁶³ CANOTILHO, J. J. Gomes; MOREIRA, Vital, op. cit., página 551.

⁶⁴ CASTRO, Catarina Sarmiento e, *O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro*, páginas 11 e 12. Disponível em, <https://egov.ufsc.br/portal/sites/default/files/anexos/5544-5536-1-PB.pdf>.

⁶⁵ NEVES, R. Castanheira, op. cit., páginas 37 e 38.

à vida contemporânea”. A delimitação do âmbito normativo deste direito toma como referências, o respeito pelos comportamentos, pelo anonimato e pela vida em relação⁶⁶.

O acórdão do Tribunal Constitucional n.º 128/92, de 24 de julho afirma que a intimidade da vida privada representa a vida pessoal, familiar, outras relações pertencentes à esfera da privacidade (amizade), os locais físicos onde as vidas mencionadas tomam lugar e os meios de expressão e comunicação, apresentando como exemplo, o correio eletrónico.⁶⁷

3.3.4. Direito à palavra

O artigo 26º da CRP autonomiza o direito à palavra, atribuindo-lhe um valor constitucional autónomo, de forma a prevenir a danosidade social a que estará sujeito, contrariamente ao que se sucede no âmbito do ordenamento jurídico alemão⁶⁸. No ponto de vista de Rita Castanheira Neves, a palavra falada é um tipo de palavra, ao qual é atribuído valor constitucional, por considerar uma maior necessidade de proteção face às características que apresenta, como uma maior volatilidade⁶⁹ e pela possível não reprodução, do que fora proferido previamente em outro contexto espaço-temporal. Assim que pronunciadas determinadas palavras, as mesmas são perpetuadas no mundo real e digital. A palavra escrita é uma tipologia mais pensada, pelo que o risco de incorrer em erro ou se comprometer é redutor, comparativamente com a palavra falada^{70 71}.

⁶⁶ CANOTILHO, J. J. Gomes/ MOREIRA, Vital, op. cit., páginas 467 e 468.

⁶⁷ Consultar em, <https://www.tribunalconstitucional.pt/tc/acordaos/19920128.html>, Ponto 13

⁶⁸ M. da Costa Andrade, *Sobre As Proibições de Prova em Processo Penal*, página 189 e 190 *apud* NEVES, R. Castanheira, op. cit., páginas 45 e 46.

⁶⁹ Para mais informações sobre as características da prova digital, RAMALHO, D. Silva, *Métodos ocultos de investigação criminal em ambiente digital*, Almedina, 2017, páginas 102 e ss.

⁷⁰ NEVES, R. Castanheira, op. cit., página 48.

⁷¹ Catarina Sarmiento e Castro realça a existência de uma terceira qualificação, denominada por palavra virtual, sendo que através desta são apresentados os conteúdos das mensagens de correio eletrónico. CASTRO, C. Sarmiento, op. cit., página 19. Conforme uma perspectiva jurídico-penal, Rita Castanheira Neves entende que a palavra virtual enquadrar-se-á na palavra escrita ou palavra falada, de acordo com as circunstâncias envolventes. Ainda que informatizada, a palavra escrita deve ser vista e tratada enquanto tal, justificando que não se compreende a razão pela qual, apenas haveria de lhe ter atribuído esse tratamento, posteriormente à impressão do conjunto das mensagens de correspondência eletrónica, NEVES, R. Castanheira, op. cit., página 50.

3.4. Regime aplicável: articulação entre o artigo 179º do Código de Processo Penal e o artigo 17º da Lei do Cibercrime

O foco desta questão versa sobre a análise do artigo 17º da LC, no qual se encontra estipulado 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 eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.”. Relativamente à parte final do artigo 17º da LC, a remissão efetuada para o regime da apreensão de correspondência corresponde aos artigos 179º e 252º⁷² do CPP⁷³.

3.4.1. A imperatividade do despacho judicial prévio

A doutrina e jurisprudência têm problematizado o papel do juiz de instrução, nesta apreensão, na fase de inquérito. Questiona-se se é imperativo a existência de uma autorização, para a apreensão de mensagens de correio eletrónico e registos de comunicações de natureza semelhante, através de despacho judicial.

⁷² MESQUITA, P. Dá, op. cit., página 118.

⁷³ Outrora à entrada em vigor da LC, já a doutrina questionava a equiparação entre a correspondência eletrónica e a correspondência física, para efeitos de regime aplicável. A doutrina maioritária defendia que a correspondência eletrónica deveria ser tratada como a correspondência tradicional. Contrariamente a esta perspetiva, Rogério Bravo considera que as mensagens recebidas num sistema informático são classificadas como dados informáticos, armazenados localmente, e que, por isso, não se equiparam ao conceito de correspondência tradicional. No ponto de vista deste autor, se o legislador tivesse intenção de estabelecer a equiparação, tê-lo-ia realizado. A introdução da expressão “intrometer no conteúdo de telecomunicação ou dele tomar conhecimento”, no artigo 194º do CP, em 1995, não pareceria justificar a equiparação, muito pelo contrário. Este artigo refere-se a mensagens que se encontram em trânsito entre o remetente e destinatário. Não só o n.º 1 consagra segmentos como, “cartas”, “escrito fechado” e “abrir carta”, referindo-se estes a encomendas fechadas, como o n.º 2, prevendo a palavra “intrometer”, reforça o pensamento do autor. Este apresenta um terceiro argumento, baseando-se na ausência de qualquer equiparação clara e expressa, entre as duas tipologias de correspondência pelo legislador ordinário. Todavia, este argumento perde vitalidade, com a remissão para o regime de apreensão do CPP, pelo artigo 17º da LC. Este ponto de vista é sufragado pela doutrina minoritária. BRAVO, Rogério, “Da não equiparação do correio eletrónico ao conceito tradicional de correspondência por carta”, *Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais*, Série III, n.º 7 (2006), páginas 207 a 213.

Pedro Verdelho considera a lei pouco clara, no que a esta problemática diz respeito. Todavia, parte da exigência de uma apreensão cautelar das mensagens, abrindo a possibilidade ao juiz de as apreender, efetivamente, quando sejam encontradas no decurso de uma pesquisa informática ou outro acesso legítimo e, se se constatar que têm interesse para a descoberta da verdade material e para a prova. O juiz de instrução recebe as mensagens, pelas mãos de quem conduz a investigação. Na eventualidade da apreensão final ser autorizada, estas são juntas ao processo. Caso contrário, serão devolvidas a quem de direito, ou destruídas, caso tenham sido feitas cópias. De acordo com este ponto de vista, a exigibilidade do despacho judicial prévio seria inexequível, uma vez que no decorrer de uma pesquisa informática, não se conhece se se encontrará computadores, se nestes existirão mensagens, e se estas terão interesse para a descoberta da verdade material e para a prova⁷⁴. Rui Cardoso partilha o mesmo posicionamento⁷⁵.

A jurisprudência⁷⁶ e doutrina maioritárias posicionam-se em sentido diverso. Sónia Fidalgo clarifica que a lei é expressa neste sentido, determinando a exigência do despacho judicial prévio⁷⁷, através, não só da interpretação da literalidade do artigo 17º da LC, como também da remissão do mesmo para o artigo 179º, n.º 1 do CPP⁷⁸. Esta é perspetiva com a qual concordo.

3.4.2. A figura do juiz, enquanto a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico

Predominantemente na fase de inquérito, o papel do juiz de instrução volta a ganhar destaque. A problemática que se levanta consiste em saber se o juiz deverá ser o primeiro a

⁷⁴ VERDELHO, Pedro, “A nova lei do cibercrime”, op. cit., páginas 743 e 744.

⁷⁵ CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei nº109/2009, de 15.IX”, op. cit., páginas 193 e 195.

⁷⁶ A este propósito, os acórdãos do Tribunal da Relação de Lisboa, de 11/01/2011 (Disponível em, <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?Op enDocument>), 05/05/2022 (Ver em, <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/97c0f4f65870d61e80258847003929a9?Op enDocument>), e o acórdão do Tribunal da Relação de Guimarães, de 29/03/2011 (Disponível em, <http://www.dgsi.pt/jtrg.nsf/c3fb530030ea1c61802568d9005cd5bb/6aa96edf91e899b2802578a00054631f?Op enDocument>).

⁷⁷ Neste sentido, NEVES, R. Castanheira, op. cit., páginas 274 e 275.

⁷⁸ FIDALGO, Sónia, op. cit., página 67.

tomar conhecimento do conteúdo mensagens de correio eletrónico, ou se esta tarefa deveria ser atribuída às entidades encarregues pela investigação.

A leitura do corpo da norma do artigo 17º da LC permite concluir pela inexistência de uma resposta direta, no que a esta problemática respeita, contrariamente à anterior. Consequentemente, a doutrina e a jurisprudência têm adotado posições diversificadas.

De acordo com a perspetiva de Pedro Verdelho, a lei não impõe que o juiz seja o primeiro a tomar conhecimento do conteúdo das mensagens de correspondência eletrónica. Atribui esta competência às entidades responsáveis pela pesquisa informática, para que posteriormente, sejam remetidas para o juiz de instrução, aquelas que tenham interesse para a prova e para a descoberta da verdade material. Este decidirá sobre o futuro das mensagens apreendidas⁷⁹.

Rui Cardoso segue a posição imediatamente anterior, apresentando um conjunto de argumentos. No seu ponto de vista, na eventualidade de a lei exigir que o juiz de instrução seja o primeiro a tomar conhecimento do conteúdo, colocar-se-ia em causa a coerência do sistema de tutela de direitos. A interseção de comunicações encontra-se prevista no artigo 18º da LC. No n.º 4, o legislador manda aplicar, em tudo o que não for contrariado pelo respetivo artigo, o regime previsto nos artigos 187º, 188º e 190º do CPP, relativo às escutas telefónicas. A letra da lei do artigo 188º, n.º 1 a 4 do CPP permite constatar pela atribuição dessa competência aos órgãos de polícia criminal. Portanto, o autor questiona a razão pela qual, o juiz de instrução possuiria a competência para tomar conhecimento do conteúdo num primeiro momento, em caso de apreensão de mensagens, sendo que este meio de obtenção de prova é menos lesivo que a interseção das comunicações. Aliado a este argumento, o autor destaca que se verificaria, não só a violação da estrutura acusatória⁸⁰, como também

⁷⁹ VERDELHO, Pedro, “A nova Lei do Cibercrime”, op. cit., página 744.

⁸⁰ O artigo 32º, n.º 5 da CRP estipula que o processo penal português apresenta uma estrutura acusatória. Vigora o princípio da acusação, o que representa a separação entre a entidade responsável pela investigação e a entidade responsável pelo julgamento, a fim de garantir a salvaguarda dos direitos fundamentais dos envolvidos, DIAS, J. Figueiredo, *Direito Processual Penal*, Coimbra Editora, Clássicos Jurídicos, Reimpressão, 2004, páginas 136 e 137. A fase de inquérito é uma fase de investigação, predominantemente. O MP é responsável pela ação penal, sendo o *dominus* do inquérito. Consequentemente, na perspetiva de Rui Cardoso, a atribuição da competência em análise ao juiz de instrução violaria a estrutura acusatória, uma vez que as mensagens apreendidas são essenciais para a investigação e para definição do objeto, o que comprometeria o papel do juiz de garantias. CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX”, op. cit., página 209. A perspetiva de RUI CARDOSO tem acolhimento na minoria da jurisprudência, destacando o acórdão do Tribunal da Relação de Lisboa, de 22/04/2021, acessível em, <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/21a767e000ff88b4802586d9002adc38?OpenDocument>.

dificuldades práticas acrescidas⁸¹, visto que são apreendidas elevadas quantidades de mensagens e o juiz de instrução não possui as ferramentas essenciais para efetuar a tarefa⁸².

A jurisprudência majoritária⁸³ não subscreve a posição *supra* apresentada. A parte final do artigo 17º da LC estipula que se aplica o regime de apreensão de correspondência previsto no CPP. Consequentemente, convocar-se-á o artigo 179º, n.º 3 do CPP, segundo o qual “O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida(...)”, perspectiva que subscrevo. A aplicação do regime de apreensão de correspondência não se restringe unicamente ao artigo 179º do CPP. O artigo 252º do CPP relaciona-se com esta temática, demonstrando o papel dos órgãos de polícia criminal, no âmbito da apreensão da correspondência tradicional. De acordo com o estipulado no artigo 252º, n.º 1 e n.º 2 do CPP, os órgãos de polícia criminal transmitem a correspondência “intacta ao juiz que tiver autorizado ou ordenado a diligência” e “sempre que tiverem fundadas razões para crer que eles podem conter informações úteis à investigação de um crime ou conduzir à sua descoberta, e que podem perder-se em caso de demora”. Estes informaram o juiz, imediatamente, para que este possa autorizar a abertura naquele momento. Concomitantemente, o artigo 252º do CPP demonstra a possibilidade de auxílio prestado pelos mesmos, a fim de colmatar as dificuldades práticas apontadas por Rui Cardoso, sem comprometer a tese, segundo a qual o juiz deve ser o primeiro a tomar conhecimento do conteúdo das mensagens de correio eletrónico⁸⁴.

O acórdão do Tribunal da Relação de Lisboa, de 7/03/2018, evidenciou que na fase de inquérito, apesar da titularidade atribuída ao MP, o juiz de instrução deve exercer as suas funções enquanto juiz de garantias e de liberdades, sempre que a circunstância implique a intromissão na esfera dos direitos fundamentais dos indivíduos, reforçando que este detém

⁸¹ Neste sentido, NEVES, R. Castanheira, op. cit., página 275.

⁸² Para uma abordagem mais extensa das suas justificativas, CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX”, op. cit., páginas 195 e ss.

⁸³ Vejamos, os acórdãos do Tribunal da Relação de Lisboa, de 11/01/2011 e 05/05/2022.

⁸⁴ Duarte A. Rodrigues Nunes convoca o artigo 252º, n.º 3 do CPP, em situações de *periculum in mora*. Este autor refuta a possibilidade de utilização do mecanismo previsto no n.º 2 do mesmo artigo, no âmbito do meio de obtenção de prova em questão. A objeção apresentada resulta das perspetivas adotadas pelo autor, em relação à exigência do despacho judicial prévio para autorizar a apreensão e à exigência de que o juiz de instrução seja o primeiro a tomar conhecimento do conteúdo das mensagens apreendidas. NUNES, D. A. Rodrigues, op. cit., página 154.

da competência para exercer todas as funções jurisdicionais⁸⁵ até à remessa do processo para a fase de julgamento. A atribuição deste papel resulta dos artigos 32º, n.º 4 e 202º, n.º 2 da CRP e 17º do CPP. Este acórdão contraria o argumento avançado por Rui Cardoso, pelo que no seu entendimento, “não colide com a estrutura acusatória do processo penal, consagrado no artigo 32º, n.º 5 da CRP, nem com a separação orgânica e funcional entre as duas magistraturas, (...), nem, muito menos, poderá ser tida como uma posição de sindicante por parte do JIC da atividade do Ministério Público.”⁸⁶. O acórdão do Tribunal Constitucional n.º 687/2021 reforçou o pensamento, estabelecendo que “a afetação de tais direitos deverá ser a menor possível, devendo limitar-se ao mínimo indispensável para assegurar uma efetiva prossecução dos bens e valores jusconstitucionais que fundamentam a restrição.”. Este conclui que das competências atribuídas pela Lei Fundamental e por outras disposições legais, ao juiz de instrução e ao MP “parece incontornável reconhecer que a intervenção judicial constitui uma garantia adicional de ponderação dos direitos e liberdades atingidos no decurso da investigação criminal.”⁸⁷. Estas justificativas valem para fundamentar a obrigatoriedade de um despacho judicial prévio, para autorizar a apreensão de mensagens de correio eletrónico, igualmente⁸⁸.

Armando Dias Ramos defende que após a extração e salvaguarda dos ficheiros informáticos, a perspetiva jurisprudencial apresentada é a mais sensata⁸⁹. Não obstante a indagação das dificuldades práticas inerentes à adoção desta perspetiva, Rita Castanheira Neves considera que a exigência de que o juiz de instrução seja o primeiro a conhecer do conteúdo, não deve ser afastada. Realça ainda que se deveria “exigir que durante a diligência se tenha sempre em atenção que, para a eficácia da mesma, devem-se seguir estritos critérios de abrangência, apenas apreendendo os emails que se afigurem realmente determinantes para a prova.”⁹⁰, a fim de solucionar o respetivo problema.

⁸⁵ Neste sentido, DIAS, J. Figueiredo, “Sobre os sujeitos processuais no novo Código de Processo Penal”, *O Novo Código de Processo Penal. Jornadas de Direito Processual Penal*, Almedina, 1995, página 16.

⁸⁶In, <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument>.

⁸⁷ Visualizar em, <https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html>.

⁸⁸ Supra, veja-se as páginas 29 e 30.

⁸⁹ RAMOS, A. Dias, op. cit., página. 107.

⁹⁰ NEVES, R. Castanheira, op. cit., página 275.

3.4.3. Acórdão do Tribunal Constitucional n.º 687/2021⁹¹

O Decreto n.º 167/XIV⁹² advém da transposição da Diretiva (EU) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019⁹³, relativa ao combate à fraude e à contrafação de meios de pagamento, que não em numerário.

O legislador português aproveitou a oportunidade, de acordo com o estipulado no artigo 5º do diploma anteriormente elencado, para alterar, não só as normas diretamente visadas pela Diretiva, como também outras que não possuem um laço direto com a mesma, tal como o artigo 17º da LC. O propósito do legislador consistia em clarificar o regime da apreensão em questão, para que se coloque um termo aos conflitos jurisprudenciais e doutrinários, gerados em torno deste artigo.

No que à proposta de alteração do artigo 17º da LC concerne, rapidamente se constata que o legislador atribui ao MP a competência para autorizar a apreensão, na fase de inquérito, uma vez que nesta, este é autoridade judiciária competente. Excepcionalmente, os órgãos de polícia criminal poderão efetuar esta tarefa, na ausência de prévia autorização da autoridade judiciária, quando esta é realizada no decurso de pesquisa informática legitimamente ordenada e executada, de acordo com o artigo 15º da LC e, quando haja urgência ou perigo na demora. No seguimento da apreensão, o MP envia as mensagens ao juiz de instrução, que decidirá acerca da junção aos autos, considerando o caso específico. Realça a aplicação, não só dos n.º 5 e n.º 8 do artigo 16º da LC, relativos à apreensão de dados informáticos, como também o estipulado na lei do CPP, acerca do regime de apreensão de correspondência, no que não se encontrar definido na proposta para o artigo 17º, desde que com as devidas adaptações. Os artigos 179º e 252º do CPP aplicar-se-ão subsidiariamente. Concomitantemente, a proposta de lei adota as posições assumidas por Pedro Verdelho e Rui Cardoso.

⁹¹ Disponível em, <https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html>.

⁹² Consultar em, <https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c6379395953565a4d5a5763765247396a6457316c626e52766330466a64476c32615752685a47565159584a735957316c626e52686369396d4e6a566b5a5751795a6930355a5459354c54526c4d3249744f444d785a533169596a4d784d6a4e6b5a54597a4d5449755a47396a65413d3d&fich=f65ded2f-9e69-4e3b-831e-bb3123de6312.docx&Inline=true>.

⁹³ Disponível em, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0713&from=PT>.

Em sede parlamentar, a proposta de lei foi avaliada, tendo sido emitido parecer pela Comissão Nacional de Proteção de Dados. Esta considera que a proposta de lei apresentada, “desprotege excessivamente as pessoas eventualmente suspeitas ou que tenham incidentalmente interagido com esses suspeitos, sendo que a exigência de intervenção do juiz de instrução, nos mesmos termos do artigo 179º do CPP, nunca pode ser vista como desvirtuadora do princípio acusatório que preside ao processo penal em Portugal”⁹⁴. A Comissão conclui, convocando o acórdão do Tribunal de Justiça da União Europeia, de 2 de março, no processo C-746/18, de forma a provar o afastamento da intervenção do MP, sem prévia autorização judicial⁹⁵. No momento posterior à aprovação pela Assembleia da República, o decreto foi enviado para o Presidente da República, para possível promulgação ou veto, nos termos dos artigos 134º, alínea b) e 136º, n.º 1 da CRP. Este solicitou a fiscalização preventiva da constitucionalidade das normas do artigo 5º do decreto, relativas ao artigo 17º da LC, ao Tribunal Constitucional, de acordo com o estipulado nos artigos 278º, n.º 1 da CRP. Considerou que as alterações apresentadas violariam os artigos 18º, n.º 2, 34º, n.º 4 e 35º da CRP.

Num primeiro momento, o Tribunal Constitucional questiona-se se seria admissível a restrição de direitos fundamentais, como o sigilo das comunicações e de outros meios de comunicação privada, estipulados no artigo 34º, n.º 1 da CRP, e a proteção de dados pessoais no âmbito da utilização da informática, previstos nos artigos 35º, n.º 1 e n.º 4 da CRP. Ressalva-se que os direitos elencados constituem refrações do direito à reserva da intimidade da vida privada e familiar, consagrado no artigo 26º da CRP. Sendo a resposta afirmativa, num segundo momento, questiona-se se as competências atribuídas ao MP e ao juiz de instrução cumprem as exigências político-constitucionais, do artigo 32º, n.º 4 da CRP e os princípios da necessidade e da proporcionalidade, do artigo 18º, n.º 2 da CRP. Responde negativamente a ambas. Por conseguinte, o Tribunal Constitucional pronuncia-se pela inconstitucionalidade das normas, por violação dos artigos 18º, n.º 2, 26º, 32º, n.º 4, 34º, n.º 1 e 35º, n.º 1 e n.º 4 da CRP⁹⁶.

⁹⁴

Disponível

em,

<https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=110841>.

⁹⁵

Disponível

em,

<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62018CJ0746&from=pt>.

⁹⁶ Rui Cardoso caracteriza a posição adotada pelo Tribunal Constitucional, como “altamente problemática”, uma vez que a justificação para a declaração de inconstitucionalidade recai sobre a intervenção do juiz de instrução, unicamente. O Tribunal Constitucional faz depender da entidade que decide, a proporcionalidade exigida ao meio de obtenção de prova, determinando que a intervenção do juiz de instrução

3.4.4. (In)exigibilidade de punição com pena de prisão superior, no seu máximo, a 3 anos

Como referido *supra*, o artigo 17º da LC remete para o regime da apreensão da correspondência estipulado no artigo 179º do CPP. No que a esta problemática diz respeito, destaca-se o n.º 1, alínea b), deste último artigo, segundo o qual o juiz pode autorizar ou ordenar a apreensão através de despacho, quando haja fundadas razões para se considerar que no caso específico, se verifique a prática de um crime punível com pena superior a 3 anos, no seu máximo. Portanto, questiona-se se a intenção legislativa passaria pela restrição a este leque de crimes.

Sónia Fidalgo e Rita Castanheira Neves⁹⁷ referem que a intenção do legislador não consiste em restringir o elenco de crimes, nos quais fosse possível a utilização da apreensão de mensagens de correio eletrónico. Isto é, o artigo 179º, n.º 1, alínea b) do CPP não teria aplicação no âmbito deste meio de obtenção de prova⁹⁸. A LC prevê o âmbito de aplicação no artigo 11º, no qual se consagra que as disposições processuais aplicar-se-ão a processos relativos a crimes previstos na LC (alínea a)), a crimes cometidos por meio de um sistema informático (alínea b)) e a crimes, em que seja essencial a recolha de prova informática (alínea c)). Conclui-se que o legislador permitiu a admissibilidade deste meio de obtenção de prova em crimes, cujas penas de prisão são inferiores a 3 anos, no seu máximo, tais como o “Dano relativo a programas ou outros dados informáticos” (artigo 4º), o “Acesso ilegítimo” (artigo 6º), a “Interseção ilegítima” (artigo 7º) e a “Reprodução ilegítima de programa protegido” (artigo 8º). A letra do artigo 11º excetua os artigos 18º e 19º, relativos à interseção de comunicações e ações encobertas, respetivamente, pelo que estes meios de obtenção de

é aquela que pode satisfazer as exigências político-constitucionais. Todavia, aos olhos deste autor, tal como mencionado previamente, esta constatação coloca em causa a estrutura acusatória do processo penal (artigo 32º, n.º 5 da CRP), na medida em que transformaria o juiz das garantias em “juiz purificador investigador”. Não só o MP é o *dominus* da fase de inquérito, como este não está isento de atuar conforme a lei, a fim de garantir a defesa dos direitos fundamentais. Se a sua atuação se rege pelos critérios de legalidade e objetividade (artigo 219º, n.º 1 da CRP e artigos 2º, 3º, n.º 2, 4º, n.º 1, alínea d) do EMP), este detém do dever de colocar em prática, o princípio da proporcionalidade em sentido amplo (artigo 18º, n.º 2 da CRP). CARDOSO, Rui, “A apreensão de correio eletrónico após o Acórdão do Tribunal Constitucional n.º 687/2021: do juiz das liberdades ao juiz purificador investigador?”, *Revista Portuguesa de Direito Constitucional*, n.º 1 (2021), páginas 153 e 154 Disponível em, <https://rpdcc.pt/wp-content/uploads/2021/12/rpdcc-ru-i-cardoso-imprensa.pdf>.

⁹⁷ NEVES, R. Castanheira, op. cit., páginas 275 e 276.

⁹⁸ Neste sentido, CORREIA, J. Conde, “Artigo 179º”, *Comentário Judiciário do Código de Processo Penal*, Tomo II, 2ª Edição, Almedina, 2020, página 650; NUNES, D. A. Rodrigues, op. cit., página 147.

prova apresentam um catálogo de crimes próprio. Se a intenção do legislador ordinário consistisse em restringir o âmbito de aplicação do meio de obtenção de prova em estudo, tê-lo-ia referido expressamente⁹⁹.

Sónia Fidalgo interroga-se se a apreensão de mensagens de correio eletrónico se aplicará em qualquer processo, para qualquer crime praticado, independentemente da gravidade do mesmo¹⁰⁰.

O artigo 11º da LC fornece a abertura necessária para que meio de obtenção de prova seja mobilizado em qualquer processo, independentemente da gravidade do respetivo crime, uma vez que o artigo 17º não é reconhecido pelo legislador ordinário como exceção, relativamente ao âmbito de aplicação. Mediatemente, o acórdão do Tribunal Constitucional, n.º 687/2021 pronuncia-se sobre a problemática levantada, declarando que da LC não decorre quaisquer limitações, “em termos inequívocos”, não deixando de reconhecer a inexistência de uma “norma paralela” ao artigo 9º da Lei n.º 32/2008, no qual se prevê que só poderá ser autorizada a transmissão de dados de tráfego armazenados pelos fornecedores de serviços de comunicações eletrónicas, às autoridades públicas, através do despacho fundamentado do juiz de instrução, na eventualidade de existir razões para considerar que a concreta diligência seja indispensável para a descoberta da verdade material ou para a prova, visto que a opção por outro meio de obtenção de prova tornaria impossível ou muito difícil a obtenção de prova, para a investigação, detenção e repressão de crimes graves¹⁰¹.

O direito processual penal português consiste num direito constitucional aplicado¹⁰², visto que “a conformação do processo penal traduz-se, muitas vezes, numa restrição de direitos fundamentais do arguido e de terceiros que envolve todo o regime constitucional de restrição dos direitos, liberdades e garantias”¹⁰³. A interpretação do artigo 18º da CRP destaca que, para que a restrição dos direitos, liberdades e garantias seja corretamente exequível, torna-se imperativo a verificação dos pressupostos materiais. O princípio da proporcionalidade em sentido amplo ou princípio da proibição do excesso ganha relevo, enquanto um dos três pressupostos materiais. Este princípio ramifica-se em 3 subprincípios, denominados por princípio da adequação ou idoneidade (os meios devem ser

⁹⁹ FIDALGO, Sónia, op. cit., páginas 65 e 66.

¹⁰⁰ *Idem*, página 66.

¹⁰¹ Disponível em, <https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html>, Nota 32.

¹⁰² Como designa H. Henkel *apud* DIAS, J. Figueiredo, *Direito Processual Penal*, op. cit., página 74.

¹⁰³ ANTUNES, M. João, op. cit., página 18.

adequados, de forma a obter o fim desejado), o princípio da exigibilidade ou necessidade ou indispensabilidade (o fim pretendido deve ser alcançado, com recurso a meios menos onerosos possíveis) e o princípio da proporcionalidade em sentido estrito (o meio utilizado não deve ser desproporcional ou excessivo, em relação ao fim que se pretende atingir)¹⁰⁴.

Face ao exposto, questiono se a utilização da apreensão regulada no artigo 17º da LC será sempre, não só proporcional ao fim que se pretende obter, como também o meio de obtenção de prova menos oneroso possível, independentemente da gravidade. Não existirão crimes de pequena criminalidade, em que este meio de obtenção de prova será excessivo ou mais oneroso, de entre os quais se obteria o mesmo fim? Não se requererá uma análise ao caso concreto, previamente?

3.4.5. A problemática da distinção entre correio eletrónico fechado/não lido e aberto/lido

A questão da essencialidade da atribuição de regimes diferenciados entre as mensagens de correio eletrónico ou registos de comunicação de natureza semelhantes abertos/lidos e fechados/não lidos, remota a um período anterior à entrada em vigor do artigo 189º do CPP e da LC. Não obstante o silêncio legislativo, Pedro Verdelho afirmava que este meio de obtenção de prova não se classificava como proibido (artigo 125º e 126º da CRP), e que era possível viabilizar a sua adoção. Segundo este autor, já se deveria efetuar a distinção entre mensagens abertas/lidas, às quais se atribuiria a proteção dada às cartas em papel, guardadas na gaveta, e as mensagens fechadas/não lidas, que receberiam a regulamentação do artigo 179º do CPP. De forma a justificar a diferenciação, convoca-se o argumento literal, segundo o qual o corpo da norma se refere a “qualquer outra correspondência”.¹⁰⁵

De olhos postos no presente, Costa Andrade¹⁰⁶, João Conde Correia¹⁰⁷ e Paulo Dá Mesquita¹⁰⁸ defendem a aplicação de um regime diversificado entre estes tipos de

¹⁰⁴ CANOTILHO, J. J. Gomes / MOREIRA, Vital, op. cit., páginas 392 e 393.

¹⁰⁵ VERDELHO, Pedro, “Apreensão de correio eletrónico em Processo Penal”, *Revista do Ministério Público*, n.º 100 (2004), página 158.

¹⁰⁶ ANDRADE, M. Costa, “Bruscamente no Verão Passado”, *A reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, op. cit., página 159.

¹⁰⁷ CORREIA, J. Conde, “Prova Digital: as leis que temos e a lei que deveríamos ter”, op. cit., páginas 40 e 41.

¹⁰⁸ MESQUITA, P. Dá, op. cit., páginas 118 e 119 (Nota 74).

mensagens. O regime previsto no artigo 17º aplicar-se-á às mensagens de correio eletrónico não lidas/fechadas, exclusivamente. Contrariamente a estas, no que às mensagens de correio eletrónico lidas/abertas diz respeito, o regime a aplicar consistirá no que se encontra estipulado no artigo 16º, relativamente à apreensão de dados informáticos. O MP pode ordenar a apreensão (n.º 1), sendo possível um controlo judicial posterior, quando esteja em causa dados íntimos (n.º 3). Pretende-se que o *e-mail* aberto seja visto como um documento, num normal escrito, desprovido de tutela das telecomunicações. O mesmo entendimento vale para os registos de comunicações de natureza semelhante, como os SMS, guardadas no cartão SIM (módulo de identificação do assinante), tendo sido recebidas ou expeditas¹⁰⁹. “A proteção do sigilo das comunicações (...) deve terminar quando a mensagem chega ao destinatário e o processo de transmissão se encontra concluído”. Deste modo, o destinatário tem a possibilidade de evitar a intromissão de terceiros¹¹⁰.

Rui Cardoso considera que, independentemente de as mensagens já tenham sido abertas, ou ainda permaneçam fechadas, o artigo 17º aplica-se em quaisquer circunstâncias. O acesso e posterior leitura pode ser efetuada num dispositivo eletrónico específico. Todavia, devido à falta de sincronização entre diversos dispositivos, a mesma mensagem pode permanecer como não lida, num segundo dispositivo. Para além desta justificação, um simples clique transforma um *e-mail* aberto, num *e-mail* fechado, sendo necessário considerar que os filtros relativos ao lido/não lido não existem na totalidade dos telemóveis ou sistemas de *smartphones*¹¹¹. Sónia Fidalgo partilha da mesma perspetiva, acrescentando que um simples clique transforma a realidade, em algo que não transborda verdade. Isto é, através do mesmo, uma mensagem lida/aberta converter-se-á numa mensagem não lida/fechada, destorcendo a veracidade dos factos. Portanto, o legislador ordinário confere uma tutela acrescida às mensagens eletrónicas, sejam estas fechadas/não lidas, sejam abertas/lidas¹¹². A atribuição de regimes diversificados culminará no desenvolver de dificuldades, uma vez que o regime aplicável se encontra subordinado à classificação atribuída às mensagens de correio eletrónico, cuja determinação constitui uma tarefa árdua.

¹⁰⁹ COSTA, M. Andrade, “Bruscamente no Verão Passado”, *A reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, op. cit., página 159.

¹¹⁰ CORREIA, J. Conde, “Prova Digital: as leis que temos e a lei que devíamos ter”, op. cit., página 41.

¹¹¹ CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX”, op. cit., página 186 e 187.

¹¹² FIDALGO, Sónia, op. cit., páginas 69 e 70.

Face ao exposto, a minha perspetiva versa sobre a posição defendida anteriormente. Considero que o tratamento legal atribuído às mensagens de correio eletrónico abertas/lidas e fechadas/não lidas deverá consistir no que se estipula no artigo 17º da LC. Mobilizando um argumento literal, o legislador ordinário não efetuou quaisquer distinções entre ambas¹¹³ nos artigos, o que nos leva a pressupor que o seu desejo seria que não houvesse diferenciação entre ambas e nos respetivos regimes a aplicar. O acórdão do Tribunal da Relação de Lisboa, de 7/03/2018 sustentou que “só se pode entender que o legislador tomou uma posição clara de submeter toda a “Apreensão de Correio Eletrónico e Registos de Comunicações de Natureza Semelhante” ao regime da apreensão de correspondência, independentemente de as Mensagens se encontrarem Abertas ou Fechadas, fazendo sujeitar a apreensão a autorização judicial, conforme o deixou consignado no artigo 17º da Lei do Cibercrime”¹¹⁴.

Atualmente, os novos equipamentos informáticos permitem o acesso direto às caixas de mensagens de correio eletrónico. Embora a mensagem não tenha sido aberta, nestes é possível a visualização do assunto concreto, da remetente e grande parte do conteúdo do corpo da mesma. Além disso, a abertura do e-mail não é condição necessária e suficiente para que o destinatário tenha conhecimento do conteúdo, visto que esta possa ter sido desencadeada por lapso, sem que a respetiva leitura lhe esteja diretamente associada.

Mesmo que a tutela conferida pelo artigo 34º, n.º 1 e n.º 4 termina-se no momento que estas chegam ao conhecimento do destinatário, sobre estas continuará a recair a tutela conferida pelos artigos 26º, 35º da CRP, entre outros. Uma vez que a restrição de direitos fundamentais se encontrará patente, mesmo em sede de fase de inquérito, nos termos do artigo 32º, n.º 4 da Lei Fundamental, o juiz de instrução deve ter um papel preponderante, num primeiro momento, tal como lhe é atribuído pelo artigo 17º da LC, e contrariamente ao que sucede no artigo 16º da LC.

¹¹³ CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX”, op. cit. página 184.

¹¹⁴ Disponível em, <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument>.

4. CONHECIMENTOS FORTUITOS

4.1. Distinção entre conhecimentos de investigação e conhecimentos fortuitos

Pela primeira vez, a Lei n.º 48/2007, 29 de agosto, proporcionou a consagração da temática dos conhecimentos fortuitos, no artigo 187º, n.º 7 e respetivo formalismo, no n.º 8 do CPP, do capítulo IV, respeitante às escutas telefónicas, exclusivamente. É de notar que, precedentemente à previsão legislativa, a doutrina e a jurisprudência já reconheciam a admissibilidade de valoração dos conhecimentos fortuitos, no âmbito deste meio de obtenção de prova, não obstante o silêncio da lei¹¹⁵.

Os conhecimentos fortuitos em sentido amplo ramificam-se em conhecimentos de investigação e conhecimentos fortuitos *stricto sensu*¹¹⁶. Presentemente, esta distinção é consensual¹¹⁷ e admitida quer, pelo plano categorial, quer pelo plano jurídico-normativo¹¹⁸.

Os conhecimentos de investigação são aqueles que poderão ser utilizados, ou no mesmo processo, ou em outros processos, desde que passíveis de serem apensos. A sua utilização não está dependente de uma nova autorização pelo juiz, tendo como condição necessária e suficiente a autorização concedida previamente, para que se mobilizasse a escuta telefónica vigente. Para além de constituírem a prova ou notícia do crime naquele processo, os conhecimentos de investigação podem constituir o objeto da investigação, possibilitando o alargamento, a restrição e modificação dos factos¹¹⁹. Portanto, a valoração de conhecimentos de investigação consiste no “aproveitamento dos dados para a prova de

¹¹⁵ Como se analisará *infra*, nas páginas 42 e ss.

¹¹⁶ Atualmente, embora a fronteira entre conhecimentos de investigação e conhecimentos fortuitos se encontre demarcada, Costa Andrade e Francisco Aguilár expuseram os seus entendimentos relativamente a este tópico, quando a diferenciação entre ambos não se encontrava destrinchada na sua plenitude. Ver em, ANDRADE, M. Costa, *Sobre As Proibições de Prova Em Processo Penal*, Reimpressão, Coimbra Editora, 2013, páginas 305 e 306; AGUILAR, Francisco, *Dos conhecimentos fortuitos obtidos através de escutas telefónicas. Contributo para o seu estudo nos Ordenamentos jurídicos Alemão e Português*, Almedina, 2004, página 21 a 24.

¹¹⁷ Veja-se, o acórdão do Tribunal da Relação de Lisboa, de 11/10/2007. Disponível em, <http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/3b5960f74cbc44a18025738b006cef87?OpenDocument>.

¹¹⁸ COSTA, M. Andrade, “O regime dos conhecimentos da investigação em processo penal”, *Revista de Legislação e de Jurisprudência*, n.º 3981 (2013), página 353.

¹¹⁹ MILHEIRO, T. Caiado, “Artigo 187º”, *Comentário Judiciário do Código de Processo Penal*, Tomo II, Almedina, 2019, páginas 761 e 762.

crimes diferentes, daquele que motivou e justificou a escuta, mas que mantêm com ele uma estreita e incindível conexão”¹²⁰.

Os conhecimentos fortuitos consistem no conjunto de dados ou informações, que poderão ser mobilizados no âmbito de outro processo diferente do qual são originários, tendo sido obtidos com recurso a escutas telefónicas validamente executadas. A transferência de dados entre processos encontra-se depende da verificação da possibilidade de efetuar, validamente as escutas telefónicas, no segundo processo. Justifica-se pelo facto de a sua utilização possuir em vista um fim diverso. Esta tipologia de conhecimentos pressupõe a inexistência de conexão entre estes e o crime, que determinou as escutas telefónicas no primeiro processo. A valoração dos conhecimentos fortuitos designa-se pelo “aproveitamento dos dados na investigação de outros crimes e no contexto de outro processo criminal, distinto daquele em que se produziram as Escutas.”. A definição dos conhecimentos fortuitos resulta do princípio da intromissão sucedânea hipotética, tal como se referem a doutrina e jurisprudência alemã¹²¹.

4.2. Considerações à luz das jurisprudências e das doutrinas alemã e portuguesa, anteriores à Lei n.º 48/2007, de 29 de agosto

Até à entrada em vigor da Lei nº48/2007, de 29 de agosto depreendemo-nos com um aumento exponencial das situações reconduzíveis à valoração dos conhecimentos fortuitos. Esta constatação obrigou a que se apresentassem soluções jurídicas, por parte da doutrina e jurisprudência nacionais e internacionais, aos variadíssimos processos instaurados.

Passo, então, a apresentar algumas considerações tomadas pelas doutrinas e jurisprudências alemã e portuguesa.

¹²⁰ ANDRADE, M. Costa, “Bruscamente no Verão Passado”, *A reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, op. cit., página 174.

¹²¹ *Idem*, página 174 a 177.

4.2.1. Jurisprudência e doutrina alemãs

Os contributos da doutrina e jurisprudência alemãs constituem a influência de excelência das soluções concedidas em Portugal, nomeadamente as relacionadas com a clarificação da admissibilidade e regime processual inerente aos conhecimentos fortuitos.

Em 1973, o OLG Hamburg enunciou que a validade das escutas telefónicas, das quais se obtém os dados a transferir para outro processo, é a condição necessária e suficiente para a admissibilidade da valoração num segundo processo¹²². Pela primeira vez, o Tribunal Federal Alemão apresentou os fundamentos que constituem o enquadramento doutrinal e normativo desta temática, através da prolação da decisão de 15 de março de 1976. Contrariamente ao OLG Hamburg, o BGH considerou que a valoração seria admissível, se os factos obtidos através das escutas telefónicas apresentassem uma relação de conexão, com a suspeita de crime de catálogo, conforme ao 100a) da StPO. Concomitantemente, para além de se proibir a valoração de conhecimentos fortuitos, quando o crime não se encontre em conexão com um crime elencado no catálogo respetivo, o Tribunal Federal chama à colação o princípio da proporcionalidade, que permite avançar que a compressão dos direitos fundamentais será admitida, nas proporções estritamente necessárias para salvaguardar bens jurídicos igualmente reconhecidos pela Constituição. A valoração dos dados insignificativos é proibida¹²³.

Posteriormente à decisão de 1976, BGH concluiu pela inexistência da obrigatoriedade de que o crime sobre o qual versa os conhecimentos fortuitos, apresente uma relação de conexão com um crime de catálogo que originou a escuta telefónica. Nada obsta a que o crime em concreto seja o mesmo que justificou a utilização das escutas telefónicas, no primeiro processo, ou que pertença ao respetivo catálogo de crimes¹²⁴. Com a decisão de 30/08/1978 do BGH, o alargamento seguinte mostrou-se inerente à verificação de crimes de terrorismo e àqueles que constituem a “finalidade ou atividade da associação criminosa”. Acrescenta-se que, na eventualidade de se determinar que a acusação pelo crime de associação criminosa seja infundada na fase de julgamento, tal facto não constitui

¹²² Decisão de 1973 do OLG Hamburg *apud* ANDRADE, M. Costa, *Sobre as Proibições de Prova em Processo Penal*, op. cit., página 307.

¹²³ Decisão 15/03/1976 do BGH Alemão *apud* ANDRADE, M. Costa, *Sobre as Proibições de Prova em Processo Penal*, op. cit., páginas 307 e 308.

¹²⁴ RIESS, “Anmerkung (BGH, 26, 298; 27, 355; 28, 122)”, *JR* 1979, páginas 165 e seguintes *apud* ANDRADE, M. Costa, *Sobre as Proibições de Prova em Processo Penal*, op. cit., 308.

impedimento para a valoração dos conhecimentos fortuitos, relativos a esta tipologia de crimes.¹²⁵

Um conjunto restrito de autores reiteram a possibilidade de valoração de conhecimentos fortuitos, sem mais¹²⁶, enquanto a expressão da tese da inadmissibilidade da valoração dos mesmos, com justificativa no princípio da reserva de lei¹²⁷, alberga uma expressão diminutamente considerável. A doutrina maioritária verte no exato sentido que a maioria da jurisprudência. Portanto, exige que o tipo de ilícito constitua um crime de catálogo. Parte da doutrina considera que esta última condição não é suficiente, para a qual haveria de se acrescentar a verificação de um requisito adicional, que se traduz na prevalência do princípio da proporcionalidade, entre a proteção dos direitos fundamentais e a descoberta da verdade e realização da justiça, através das escutas telefônicas. A doutrina inclina-se para compreender os conhecimentos fortuitos, em torno do juízo hipotético de intromissão, em que recaem sobre os mesmos um estado de necessidade investigatório¹²⁸.

4.2.2. Jurisprudência e doutrina portuguesas

Aliada à exigência de que o crime associado aos conhecimentos fortuitos obtidos se reporte ao catálogo estipulado no artigo 187º, n.º 1 do CPP, a doutrina imponha a obrigatoriedade de se “reproduzir aquele estado de necessidade investigatório que o legislador terá arquetipicamente representado como fundamento da legitimação das escutas telefônicas”. A presença de crimes que integram a finalidade ou atividade de associação criminosa não representa qualquer infortúnio para a valoração dos conhecimentos fortuitos, como prova ou notícia do crime¹²⁹.

O acórdão do Supremo Tribunal Justiça, de 23/10/2002 acompanhou a perspectiva de Costa Andrade, afirmando que esta se demonstra “suficientemente cautelosa e não afrontadora da lei”. Reconheceu que o aproveitamento dos conhecimentos fortuitos será

¹²⁵ Decisão de 30/08/1978 do BGH Alemão *apud* ANDRADE, M. Costa, *Sobre as Proibições de Prova em Processo Penal*, op. cit., páginas 308 e 309.

¹²⁶ Como defende, W. SCHUNEMANN *apud* ANDRADE, M. Costa, *Sobre as Proibições de Prova em Processo Penal*, op. cit., página 309.

¹²⁷ Como perspectiva, PRITTWITZ *apud* ANDRADE, M. Costa, *Sobre as Proibições de Prova em Processo Penal*, op. cit., página 309.

¹²⁸ Afirmando por RUDOLPHI *apud* ANDRADE, M. Costa, *Sobre as Proibições de Prova em Processo Penal*, op. cit., página 310.

¹²⁹ ANDRADE, Manuel Costa, *Sobre proibições de prova*, op. cit., página 311 e 312.

válido, se se fizer cumprir requisitos específicos. Passo a enumerar os requisitos apontados pelo acórdão: as escutas telefónicas, nas quais os conhecimentos fortuitos têm origem, devem obedecer à totalidade dos requisitos consagrados no artigo 187º, n.º1 do CPP, de forma que estas sejam válidas; o crime sobre o qual se obtém informações, deve constituir-se como crime de catálogo; a valoração dos conhecimentos fortuitos deve comportar uma importância tal para a descoberta da verdade material e para a prova, no processo para o qual o transporte é executado e o direito ao contraditório do arguido deve-lhe ser concedido¹³⁰.

4.3. Valoração dos conhecimentos fortuitos, no âmbito das escutas telefónicas, à luz da Lei n.º 48/2007, de 29 de agosto

Nos termos do artigo 187º, n.º 7 do CPP, “sem prejuízo do artigo 248º, a gravação de conversações ou comunicações só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no n.º 4 e na medida em que for indispensável à prova de crime previsto no n.º 1.”. No seguimento desta norma, o n.º 8 acrescenta que, mediante despacho do juiz, os suportes técnicos das conversações ou comunicações e despachos que justificaram as interseções são juntos ao segundo processo, àquele onde serão valorados como prova. As cópias são extraídas, na eventualidade de o ser desejável.

Face ao exposto na lei processual penal, a “transferência” e consequente valoração de determinadas informações obtidas no âmbito de um processo diversificado pressupõe a verificação de requisitos, cumulativamente. Estes são: os conhecimentos fortuitos tenham resultado de escutas telefónicas válidas; a migração diga respeito a provas obtidas, que se reportem a um crime de catálogo, previsto no artigo 187º, n.º 1 do CPP; nas circunstâncias do caso concreto, devem existir razões, para que os conhecimentos fortuitos sejam indispensáveis para provar os factos, que se reconduzem à prática do tipo de ilícito; é igualmente imperativo que os conhecimentos fortuitos resultem da interseção do meio de comunicação utilizado pelas pessoas elencadas no artigo 187º, n.º 4 do CPP, e, por último, o n.º 8 do artigo 188º estipula a exigibilidade de um despacho do juiz, a fundamentar a

verificação ou ausência dos pressupostos para a transmissão dos conhecimentos fortuitos, para o segundo processo. A inobservância de qualquer requisito é condição suficiente para que a valoração dos conhecimentos fortuitos seja inexequível, sendo esta prova proibida¹³¹.

4.3.1. 1º Requisito: obtenção de conhecimentos fortuitos, a partir de escutas telefônicas válidas, no âmbito do primeiro processo

As escutas telefônicas consistem num dos meios de obtenção de prova mais intrusivos, nos direitos fundamentais dos intervenientes, o que justifica o regime estabelecido pelo legislador, de forma a promover a concordância prática entre as finalidades processuais e a efetivar o estipulado pelo princípio da proporcionalidade, artigo 18º, n.º 2 da CRP¹³². O regime aplicável aquando da mobilização da interseção e da gravação de conversações ou comunicações telefônicas encontra-se estipulado ao longo do artigo 187º do CPP. No n.º 1 do respetivo artigo, evidencia-se que este meio de obtenção de prova poderá ser mobilizado, unicamente, durante a fase de inquérito, a requerimento do MP, apresentado ao juiz de instrução, sendo que este, deverá averiguar acerca da sua admissibilidade, pronunciando-se através de um despacho judicial prévio fundamentado (artigo 269º, n.º 1, alínea e) do CPP). Acresce que a mobilização das escutas telefônica encontra-se dependente, não só de que o crime em investigação corresponda a um dos que se encontra elencado nas vastas alíneas no n.º 1 e n.º 2 (nos crimes elencados neste último, denota-se a particularidade de que, a autorização pode ser pedida ao juiz do lugar, onde se puder efetivar a conversação telefônica ou da sede da entidade que possua competência para investigar), como também da existência de razões para considerar que estas são indispensáveis para a prova, que de outra forma não seria possível obtê-la ou seria muito difícil, e para a descoberta da verdade material.

Relativamente ao último requisito realçado, demonstra-se os princípios da subsidiariedade, necessidade, adequação e proporcionalidade em sentido estrito. De acordo com o juízo de prognose, deseja-se que a diligência cumpra o objetivo traçado. “O recurso às Escutas Telefônicas só será admissível quando houver razões objetiva e judicialmente controláveis que permitam concluir que já foram utilizados malogradamente outros meios

¹³¹ MILHEIRO, T. Caiado, “Artigo 187º”, op. cit., páginas 762 e 763.

¹³² Veja-se as páginas 22 e ss.

de prova, ou que o recurso às escutas telefónicas (mesmo que o primeiro a ser usado) é o mais eficaz, atendendo à natureza do crime e às circunstâncias.”. Este é o raciocínio considerado, uma vez que normalmente, a prevalência é cedida aos meios de obtenção de prova menos intrusivos. O princípio da adequação ganha dimensões, na medida em que se pretende que, as escutas telefónicas sejam idóneas à recolha de prova¹³³.

O artigo 187º, n.º 4 da CPP estabeleceu a limitação subjetiva, circunscrevendo o núcleo de indivíduos que compõem o conjunto, contra qual a interseção e a gravação possa ser autorizada, independentemente do titular do meio de comunicação mobilizado. O conjunto é constituído pelo “suspeito e arguido”, (alínea a)), “pessoa que sirva de intermédio, relativamente à qual haja fundada razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido”, (alínea b)) “vítima de crime, mediante o respectivo consentimento, efetivo ou presumido”, (alínea c)). Esta delimitação fora estabelecida com a Lei n.º 48/2007, de 29 de agosto, pelo que previamente à revisão, qualquer pessoa poderia ser considerada.¹³⁴

Todavia, o artigo 187º, n.º 4 do CPP acarreta consigo determinadas problemáticas, nomeadamente, associadas ao artigo 187º, n.º 7 do CPP, pelo que será abordado *infra*¹³⁵ ¹³⁶.

4.3.2. 2º Requisito: as provas obtidas, que constituem os conhecimentos fortuitos, reportam-se a um crime de catálogo

De acordo com o entendimento pacífico, os conhecimentos fortuitos obtidos através das escutas telefónicas, no primeiro processo, devem-se referir a provas que provem os factos reconduzíveis a um crime específico. No segundo processo, a sua respetiva valoração encontra-se dependente do facto de este crime se enquadrar no n.º 1 do artigo 187º do CPP¹³⁷,

¹³³ LEITE, A. Lamas, “As escutas telefónicas – algumas reflexões em redor do seu regime e das consequências processuais derivadas da respetiva violação”, *Revista da Faculdade de Direito da Universidade do Porto*, 2004, página 26 e 27.

¹³⁴ SILVA, G. Marques da, *Curso de Processo Penal*, Vol. II, 5ª Edição, Revista e atualizada, Editora Verbo, páginas 296 e 297.

¹³⁵ Veja-se as páginas 48 e 49.

¹³⁶ Para mais entendimentos quando aos requisitos exigíveis para a admissibilidade das escutas telefónicas, VALENTE, M. M. Guedes, *Escutas Telefónicas – da Excepcionalidade à Vulgaridade*, 2ª Edição, Coimbra Editora, páginas 57 e ss; LOPES, J. Mouraz, “Escutas Telefónicas: seis teses e uma conclusão”, *Revista do Ministério Público*, n.º 104 (2005), páginas 139 e ss.

¹³⁷ ANDRADE, M., “Bruscamente no Verão Passado”, *A reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, op. cit., página 178.

tal como subscreve o artigo 187º, n.º 7 do CPP. Isto é, crimes “puníveis com pena de prisão superior, no seu máximo a 3 anos” (alínea a)), “relativos ao tráfico de estupefacientes” (alínea b)), “de detenção de arma proibida e de tráfico de armas” (alínea c)), “de contrabando” (alínea d)), “de injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone” (alínea e)), “de ameaça com prática de crime ou de abuso e simulação de sinais de perigo” (alínea f)) e “de evasão, quando o arguido haja condenado por algum dos crimes” previstos anteriormente (alínea g)). Não obstante a existência de um segundo catálogo no n.º 2 do artigo 187º do CPP, o n.º 7 remete para n.º 1, exclusivamente.

No primeiro processo, a queda do crime originário não constitui obstáculo à valoração dos conhecimentos fortuitos, independentemente da fase processual na qual se encontraria, sendo substituído pelo crime subsequente, “para assegurar a continuidade da legitimação que a lei associou àquela exigência¹³⁸.”

4.3.3. 3º Requisito: âmbito subjetivo considerado pelo artigo 187º, n.º 7 do CPP

Como mencionado *supra*, o artigo 187º, n.º 4 apresenta-se como sendo uma norma problemática, quando relacionada com o artigo 187º, n.º 7 do CPP. Os órgãos de polícia criminal, responsabilizados pela gravação da comunicação, têm o dever de averiguar se os visados são os mesmos, sobre o qual versa o despacho judicial, que autoriza a escuta telefónica. Na eventualidade de o indivíduo não constar da autorização, a interseção e gravação não podem ser efetuadas. O artigo 188º, n.º 6, alínea a) estipula que, caso se tenha procedido à elaboração de suportes técnicos e relatórios, e o visado não conste do n.º 4 do artigo 187º do CPP, o juiz deve destruí-los, imediatamente. Todavia, o artigo 187º, n.º 7 do CPP constitui uma ressalva. Nos termos do n.º 7, quaisquer pessoas poderão ser as visadas pela gravação de conversações¹³⁹, isto é, “estas conversações ou comunicações podem ser de pessoa diversa daquela relativamente a quem a escuta foi ordenada, bastando que o meio de comunicação seja utilizado pela pessoa a quem a escuta se refere.”. Portanto, os conhecimentos fortuitos poderão dizer respeito, não só a pessoas que são visadas pela escuta

¹³⁸ ANDRADE, M. Costa, “Bruscamente no Verão Passado”, *A reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e que devia ter sido diferente*, op. cit., página 178.

¹³⁹ SILVA, G. Marques da, op. cit., páginas 297 e 298.

autorizada, no primeiro processo, como também a indivíduos diversos, na condição de estes utilizarem os meios de comunicação das primeiras e a interseção tenha sido aprovada pelo juiz de instrução.¹⁴⁰

4.3.4. 4.º Requisito: a indispensabilidade da valoração dos conhecimentos fortuitos, para provar os factos reconduzíveis à verificação do tipo de ilícito

Nos termos avançados pelo artigo 187º, n.º 7 do CPP, a valoração de gravações de conversações ou comunicações em processo diverso daquele no qual tiveram origem, é admissível, na condição se esta ser indispensável à prova dos factos reconduzíveis ao tipo de ilícito. A perspetiva demonstrada pelo legislador ordinário pretende expor que a valoração dos conhecimentos fortuitos seja necessária, e o único meio possível, dentro de um leque vasto de meios de obtenção de prova e meios de prova, para provar a verificação do crime em investigação, no segundo processo. Isto, sem prejuízo da essencialidade da manutenção da proporcionalidade entre a descoberta da verdade material e a realização da justiça e da salvaguarda dos direitos fundamentais. Por conseguinte, o legislador volta a consagrar o princípio da subsidiariedade e o princípio da proporcionalidade em sentido amplo, nos três subprincípios¹⁴¹, como se considera no âmbito da admissibilidade de qualquer escuta telefónica.

Esta constatação é retirada da exposição de Costa Andrade, ao mencionar que a utilização e valoração de conhecimentos fortuitos obtidos através de escutas telefónicas válidas, seja admitida se se “justificasse, só por si (...)o recurso às escutas telefónicas.”. Reporta-se, portanto, nas palavras deste autor, ao “princípio da intromissão sucedânea hipotética”¹⁴².

¹⁴⁰ SILVA, G. Marques, op. cit., página 307.

¹⁴¹ Veja-se as páginas 37 e 38.

¹⁴² ANDRADE, M. Costa, “Bruscamente no Verão Passado”, *A reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, op. cit., páginas 173 e 174.

4.3.5. 5.º Requisito: a prolação do despacho judicial a autorizar a transmissão dos conhecimentos fortuitos, para o segundo processo

A valoração dos conhecimentos fortuitos, num processo distinto daquele que lhes deu origem, carece de validação jurisdicional através de despacho, pelo juiz do processo de origem. Previamente à transferência entre processos, o juiz efetua uma avaliação autónoma, de forma a averiguar a satisfação dos requisitos exigidos. Contrariamente ao que a letra do artigo 187º, n.º 1 menciona, o n.º 8 não especifica o juiz em questão. Pressupõe-se, portanto, a abertura para que, quer o juiz de instrução, quer o juiz de julgamento, tenham competência. O último possui esta competência, quando os conhecimentos fortuitos têm origem em interseções que não se tenham destruído e a relevância dos mesmos se tenha demonstrado na fase de julgamento, por exemplo¹⁴³.

O pedido dirigido ao juiz do primeiro processo, pode ser emitido pelo MP, na fase de inquérito, pelo juiz de instrução, na fase de instrução, ou pelo juiz de julgamento, na fase de julgamento do processo, onde a valoração dos conhecimentos fortuitos tomará lugar. Do pedido efetuado ao juiz, deve constar a identificação do crime considerado no segundo processo e as razões pela qual, a valoração dos conhecimentos fortuitos é indispensável para provar a realidade fáctica¹⁴⁴.

4.4. Aproveitamento de correspondência eletrónica, no processo penal, já apreendida e valorada à ordem de outro processo

Exclusivamente, a temática dos conhecimentos fortuitos consta do artigo 187º, n.º 7 do CPP, no que às escutas telefónicas concerne. A apreensão de mensagens de correio eletrónico e registos de comunicações de natureza semelhante apresenta um regime específico, no qual é inexistente quaisquer referências à valoração dos conhecimentos fortuitos. A problemática fulcral para o presente estudo consiste em compreender da admissibilidade da valoração dos conhecimentos fortuitos, no seio deste meio de obtenção de prova, isto é, averiguar da possibilidade de valoração de mensagens de correio eletrónico

¹⁴³ MILHEIRO, T. Caiado, “Artigo 187º”, op. cit., página 763.

¹⁴⁴ *Idem*, páginas 763 e 764.

num segundo processo, tendo estas sido previamente apreendidas, individualizadas e valoradas, num primeiro processo, não obstante o silêncio da lei.

Manuel Guedes Valente demonstra a adoção da tese, segundo a qual é possível a admissibilidade de valoração de conhecimentos fortuitos obtidos, no âmbito de conversações e comunicações estabelecidas pelo correio eletrónico. Apresenta como sua base, os pensamentos avançados no âmbito das escutas telefónicas¹⁴⁵.

Sónia Fidalgo admite a possibilidade de aplicação do regime geral dos conhecimentos fortuitos. A inexistência de qualquer previsão expressa na lei não é impedimento direto para que o aproveitamento de dados de investigação de outros crimes, num processo penal distinto daquele em que a apreensão teve lugar, não seja possível. Na sua perspetiva, valerá o que fora defendido pela doutrina e pela jurisprudência, em momentos anteriores ao silêncio legislativo¹⁴⁶.

Rui Cardoso partilha da posição imediatamente anterior. O autor afirma que, caso não se verifique restrições no âmbito objetivo ou subjetivo quanto ao concreto meio de obtenção de prova, a migração da prova verificar-se-á sem limitações, pressupondo que a mesma tenha sido originalmente obtida de forma válida. Igualmente, convoca as perspetivas avançadas pela doutrina e pela jurisprudência, anteriormente à revisão de 2007. Este autor avança com um regime, que consistirá no seguinte. No primeiro processo, as mensagens de correio eletrónico são encontradas armazenadas no sistema informático ou noutra, a que fosse possível aceder a partir do primeiro, tendo sido obtidas através de uma válida pesquisa informática ou acesso legítimo a um sistema informático. As mensagens apreendidas podem valer para provar os factos reconduzíveis a qualquer crime, uma vez que em abstrato não há um catálogo de crimes¹⁴⁷ (artigo 11º, n.º 1 da LC). Além disso, o remetente ou destinatário poderão consistir em qualquer pessoa, visto que não se limita o âmbito subjetivo. No ponto

¹⁴⁵ VALENTE, M. M. Guedes, op. cit., página 127.

¹⁴⁶ FIDALGO, Sónia, op. cit., páginas 70 e 71.

¹⁴⁷ Rui Cardoso desconsidera que a admissibilidade da temática dos conhecimentos fortuitos, no seio da apreensão da correspondência eletrónica, obedeça à aplicação analógica do artigo 187º, n.º 7 do CPP, devido à inexistência do catálogo de crimes. CARDOSO, Rui, “Apreensão de mensagens de correio eletrónico e de natureza semelhante”, *Direito Probatório, Substantivo e Processual Penal*, Centro de Estudos Judiciários, 2019, página 96. Disponível em, <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=Rj-un6PLgHo=&portalid=30>.

de vista deste autor, a autorização para o aproveitamento probatório será sempre do magistrado do MP^{148 149}.

Ao longo dos últimos anos, a jurisprudência portuguesa já se tem debruçado sobre esta problemática, nomeadamente no acórdão do Tribunal da Relação de Lisboa, de 11/07/2019. Na fase de inquérito, o MP do segundo processo, solicitou a autorização ao juiz de instrução, de cada um dos processos de origem, para proceder a uma nova pesquisa nas caixas de correspondência eletrónica, que já se encontravam apreendidas, para posterior apresentação ao juiz de instrução e remessa para o segundo processo. O juiz de instrução do processo de destino, do tribunal *a quo*, declarou nulo o despacho do juiz de instrução do processo de origem, por se considerar a si, como o juiz competente para conceder a autorização. Face ao exposto, o MP interpôs recurso do despacho. Quer o MP, quer o juiz de instrução do processo de destino, perspetivaram que o aproveitamento processual carece de autorização judicial. Todavia, divergem quanto ao juiz de instrução que a deva conceder. No ponto de vista do MP, o juiz de instrução dos processos de origem são os juízes competentes para averiguar da admissibilidade e conceção da autorização. Contrariamente a este sujeito processual, o juiz de instrução dos presentes autos declara-se a si, como juiz competente, a fim de autorizar o aproveitamento extraprocessual. O Tribunal da Relação de Lisboa considerou que o afastamento do regime da valoração dos conhecimentos fortuitos, estipulado no artigo 187º, n.º 7 e no n.º 8 do CPP, consiste num raciocínio tomado pelo juiz do tribunal *a quo*, erroneamente. Este considerou que, uma vez que o legislador ordinário português não estipulou quaisquer normas, no qual se admita e regule o aproveitamento extraprocessual, no âmbito da apreensão de correspondência eletrónica, não se poderia enveredar pelo artigo 187º, n.º 7 e 8 do CPP. Portanto, aos seus olhos, o meio mobilizado consistiria num meio de obtenção de prova atípico. Concomitantemente, o tribunal de 2ª instância conclui que o juiz de instrução do tribunal *a quo* não detinha da competência necessária para se pronunciar acerca da migração das mensagens de correio eletrónico, quando o juiz do processo de origem já se tinha pronunciado, quanto à respetiva legalidade.

¹⁴⁸ CARDOSO, Rui, “Apreensão de mensagens de correio eletrónico e de natureza semelhante”, *Direito Probatório, Substantivo e Processual Penal*, Centro de Estudos Judiciários, 2019, páginas 95 a 97.

¹⁴⁹ O magistrado do MP é encarregue de autorizar a migração da prova, do processo de origem para o processo de destino, no ponto de vista deste autor, o que se relaciona com a posição adotada pelo mesmo, relativamente à problemática da obrigatoriedade de despacho prévio judicial a autorizar a apreensão de mensagens de correio eletrónico e registos de comunicações semelhantes, nos termos do artigo 17º da LC. Veja-se as páginas 29 e ss.

Acrescentou que o juiz do tribunal *a quo* violou não só, o princípio do juiz natural, como também a competência exclusiva do juiz do processo de origem¹⁵⁰.

A decisão do acórdão proferido desencadeou alguma perplexão. A situação fáctica correspondia à solicitação do MP ao juiz de instrução, para efetuar uma nova pesquisa a caixas de correio eletrónico apreendidas à ordem de outro processo, o que se distingue daquilo que se denomina por conhecimentos fortuitos, que, por sua vez se designa pelo aproveitamento de mensagens de correio eletrónico apreendidas, individualizadas e valoradas, num processo distinto daquele onde se verifica a apreensão. A realização de uma nova busca informática implica que o conteúdo seja desconhecido, tal como sucede no acórdão, e contrariamente ao que sucede na temática dos conhecimentos fortuitos¹⁵¹.

Decorrida a nova pesquisa à caixa de mensagens de correspondência eletrónica, a apreensão individualizada destas deverá ser autorizada pelo juiz de instrução do segundo processo, no qual se pretende efetuar a nova pesquisa. Tal facto tem fundamento no artigo 17º da LC, sendo este aquele que ocupa uma melhor posição que permita averiguar se as mensagens em questão possuem “grande interesse para a descoberta da verdade material ou para a prova”¹⁵².

Não obstante a recondução errónea à temática dos conhecimentos fortuitos, o acórdão do Tribunal da Relação de Lisboa reconheceu a possibilidade de valoração de mensagens de correio eletrónico, apreendidas num primeiro processo, de forma a constituir prova dos factos reconduzíveis a de crime diverso, num segundo processo.

Tendo em vista o exposto, quer a nível doutrinal, quer a nível jurisprudencial, partilho da mesma perspetiva até então exposta. Portanto, considero que seja possível a migração de mensagens de correio eletrónico para um segundo processo, tendo estas sido apreendidas e individualizadas, no primeiro processo. O artigo 187º, n.º 7 do CPP confere abertura para a possibilidade de valoração dos conhecimentos fortuitos, no seio de outros meios de obtenção de prova, atribuindo-lhe assim, um carácter transversal aos mesmos. A condição consiste na adaptação do regime previsto no n.º 7, com a finalidade de garantir a proporcionalidade desejada. Concomitantemente, convoco o regime apresentado por Rui

150

Consultar

em,

<http://www.gde.mj.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1bc410315a7483298025843b004c1e71?OpenDocument>.

¹⁵¹ FIDALGO, Sónia, op. cit., páginas 71 e 72.

¹⁵² *Ibidem*.

Cardoso, modificando a parte final do seu raciocínio, na qual atribuí a competência ao MP, no processo originário, para autorizar a transferência dos conhecimentos fortuitos¹⁵³. Substituiria o MP, pelo juiz do primeiro processo, no qual as mensagens de correio eletrônico foram apreendidas e individualizadas.

Uma vez que esta circunstância obteve uma expressão mais elevada junto da doutrina e jurisprudência, o legislador tomou a iniciativa de prever esta possibilidade, no capítulo das escutas telefônicas, o que não inviabiliza que o mesmo suceda com outros meios de obtenção de prova.

Como referido *supra*, a Lei n.º 48/2007 proporcionou a alteração aos artigos 187º, n.º 7 e 189º, n.º 1 do CPP, prevendo a admissibilidade da valoração de conhecimentos fortuitos e a aplicação do regime das escutas telefônicas (no qual se inclui o artigo 187º, n.º 7 e o n.º 8 do CPP), nas comunicações ou conversações em suporte distinto de telefone, como o correio eletrônico, mesmo que se encontrem guardadas em suporte digital, respetivamente. A alteração simultânea em ambos os artigos pode representar o desejo do legislador em expandir o regime dos conhecimentos fortuitos, à realidade do correio eletrônico, quando as mensagens já se encontrassem guardadas, o que não obsta a que se considere que, o regime no artigo 187º, n.º 7 e do n.º 8 seja desadequado para este último, como mencionado *supra*.

¹⁵³ Veja-se as páginas 51 e 52.

5. CONCLUSÃO

O artigo 17º da LC consagra a apreensão de mensagens de correio eletrônico e registos de comunicações de natureza semelhante, estejam estas abertas/lidas, ou fechadas/não lidas, quando se afigurem de grande interesse para a descoberta da verdade ou para a prova. Este atribui-lhe um regime próprio, aplicando-se remissivamente, o artigo 179º e 252º do CPP. Face a esta previsão, o artigo 189º não apresenta quaisquer possibilidades de aplicação no seio deste meio de obtenção de prova, apesar do aditamento legal com a revisão de 2007.

De acordo com o artigo 11º, n.º 1 da LC, a utilização deste meio de obtenção de prova não está restringida a um catálogo de crimes específico, apesar de o artigo 179º, n.º 1, alínea b) do CPP apresentar uma restrição da sua aplicação aos processos relativos a crimes, cuja pena de prisão é superior, no seu máximo, a 3 anos. Esta limitação não se aplica nesta apreensão.

O juiz possui um papel preponderante para que a apreensão se execute, na fase de inquérito, artigo 17º do CPP e artigo 202º, n.º 1 da CRP. Para além da clareza da lei, no que à obrigatoriedade do despacho judicial prévio concerne (artigo 17º da LC e 179º, nº1 do CPP), o juiz de instrução deve ser o primeiro a tomar conhecimento do conteúdo das mensagens do correio eletrônico apreendidas (artigo 17º da LC e 179º, nº3 do CPP). Embora o MP seja a entidade responsável na fase de inquérito, o juiz de instrução, enquanto juiz das garantias e liberdades, deve executar determinados atos, como os mencionados anteriormente, quando estes contendam com os direitos fundamentais dos intervenientes, artigos 32º, n.º 4 e 202º, n.º 2 da CRP.

Apesar do silêncio legislativo, admite-se a possibilidade de migração e respetiva valoração de mensagens de correio eletrônico, no processo de destino, tendo estas sido apreendidas e individualizadas à ordem de um processo diverso. Para justificar esta pretensão, convoca-se as considerações da doutrina e da jurisprudência, em momentos anteriores à previsão legal da valoração de conhecimentos fortuitos, no âmbito das escutas telefónicas. Com a finalidade de promover a proporcionalidade exigida, a valoração dos conhecimentos fortuitos, no seio da apreensão destas mensagens, encontra-se dependente da verificação de requisitos específicos, de forma a salvaguardar os direitos fundamentais e a realização da justiça e a descoberta da verdade material. Claro se torna que os requisitos

exigíveis se diferenciam parcialmente, do que o legislador ordinário impõe para que a valoração dos conhecimentos fortuitos, no âmbito das escutas.

A admissibilidade da valoração de mensagens de correio eletrónico, num segundo processo, tendo estas sido apreendidas e valoradas, à ordem de um processo diverso, apresenta enquanto requisitos, a validade da apreensão da qual estas resultam, a sua indispensabilidade para provar a verificação dos elementos constitutivos do crime em investigação no segundo processo, e, por último, carece de um despacho prévio fundamentado do juiz do primeiro processo, no qual as mensagens foram apreendidas e individualizadas, a fim de justificar a verificação dos requisitos anteriores.

A valoração de conhecimentos fortuitos diferencia-se da realização de uma nova pesquisa informática à caixa de mensagens de correio eletrónico apreendidas num processo anterior. Esta pressupõe uma nova busca informática e conseqüente apreensão de eventuais *emails*, que para além de estes não se encontrarem individualizados, os seus respetivos conteúdos não são ainda conhecidos. Contrariamente ao que se sucede na temática dos conhecimentos fortuitos, a solicitação para a apreensão destes *emails* deve ser enviada pelo MP, ao juiz de instrução do segundo processo (aquele onde se pretende efetuar uma nova pesquisa), uma vez que este é aquele que conseguirá averiguar acerca da verificação dos requisitos, nomeadamente se estes possuem grande interesse para a descoberta da verdade e para a prova.

6. JURISPRUDÊNCIA

Acórdão da Relação de Lisboa, 11/07/2019, relatora Conceição Gonçalves, processo n.º 184/12.5TELSB-B.L1-3, acessível em <http://www.gde.mj.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1bc410315a7483298025843b004c1e71?OpenDocument>

Acórdão do Tribunal da Relação de Lisboa, 11/19/2007, relator João Carrola, processo n.º 3577079, acessível em <http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/3b5960f74cbc44a18025738b006cef87?OpenDocument>

Acórdão do Tribunal da Relação de Lisboa, 07/03/2018, relatora Conceição Gonçalves, processo n.º 184/12.5TELSB-B.B.L1-3, acessível em <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument>

Acórdão do Tribunal da Relação de Lisboa, 05/05/2022, relatora Maria José Cortes Caçador, processo n.º 305/19.7T9AGH-A.L1-9, acessível em <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/97c0f4f65870d61e80258847003929a9?OpenDocument>

Acórdão do Tribunal da Relação de Lisboa, 11/01/2011, relator Ricardo Cardoso, processo n.º 5412/08.9TDLSB-A.L1-5, acessível em <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument>

Acórdão do Tribunal da Relação de Lisboa, 22/04/2021, relator Fernando Estrela, processo n.º 184/12.5TELSB-N.L1-9, acessível em <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/21a767e000ff88b4802586d9002adc38?OpenDocument>

Acórdão do Tribunal da Relação de Guimarães, 29/03/2011, relatora Maria José Nogueira, processo n.º 735/10.0GAPTL-A.G1, acessível em <http://www.dgsi.pt/jtrg.nsf/c3fb530030ea1c61802568d9005cd5bb/6aa96edf91e899b2802578a00054631f?OpenDocument>

Acórdão do tribunal de Justiça da União Europeia, de 2/03/2021, processo n.º C-746/18, acessível em, <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62018CJ0746&from=pt>

Acórdão do Tribunal Constitucional n.º 128/92, relator Messias Bento, processo n.º 260/90, acessível em <https://www.tribunalconstitucional.pt/tc/acordaos/19920128.html>

Acórdão do Tribunal Constitucional n.º 687/2021, relatora Conselheira Mariana Canotilho, processo n.º 830/2021, acessível em <https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html>

7. BIBLIOGRAFIA

AGUILAR, Francisco, *Dos conhecimentos fortuitos obtidos através de escutas telefónicas. Contributo para o seu estudo nos ordenamentos jurídicos alemão e português*, Almedina, 2004

ANDRADE, M. Costa, *Sobre as Proibições de Prova em Processo Penal*, Reimpressão, Coimbra Editora, 2013

ANDRADE, M. Costa, “O regime dos “conhecimentos de investigação” em processo penal”, *Revista da Legislação e de Jurisprudência*, n.º 3981 (2013)

ANDRADE, M. Costa, “Bruscamente no Verão Passado”, *A reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra Editora, 2009

ANDRADE, M. Costa, “Artigo 194º”, *Comentário Conimbricense do Código Penal, Parte Especial*, Tomo I, 2ª edição, Coimbra Editora, 2012

ANTUNES, M. João, *Direito Processual Penal*, 2ª Edição, Reimpressão, Almedina, 2019

ASCENSÃO, J. de Oliveira, “O Cibercrime”, *Direito Penal Económico e Financeiro*, Coimbra Editora, 2012

BRAVO, Rogério, “Da não equiparação do correio-eletrónico ao conceito tradicional de correspondência por carta”, *Revista do Instituto Superior de polícia Judiciária e Ciências Criminais*, Coimbra Editora, n.º 7 (2006)

CANOTILHO, J. J. / MOREIRA Vital, *Constituição da República Portuguesa Anotada*, Vol. I, 4ª Edição Revista, Coimbra Editora, 2007

CARDOSO, Rui, “Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17º da Lei n.º 109/2009, de 15.IX”, *Revista do Ministério Público*, n.º 153 (2018)

CARDOSO, Rui, “A apreensão de correio eletrónico após o Acórdão do Tribunal Constitucional n.º 687/2021: do juiz das liberdades ao juiz purificador investigador?”, *Revista Portuguesa de Direito Constitucional*, n.º 1 (2021). Disponível em, <https://rpdc.pt/wp-content/uploads/2021/12/rpdc-rui-cardoso-impressao.pdf>

CARDOSO, Rui, “Apreensão de mensagens de correio eletrónico e de natureza semelhante”, *Direito probatório, Substantivo e Processual Penal*, Centro de Estudos

Judiciários, 2019. Disponível em, <https://cej.justica.gov.pt/LinkClick.aspx?fileticket=Rj-un6PLgHo=&portalid=30>

CASABONA, C. M. Romeo, *La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de la red*. Disponível online, <https://www.metodista.br/revistas/revistas-izabela/index.php/dih/article/view/135>

CASTRO, C. Sarmiento, O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro. Disponível em, <https://egov.ufsc.br/portal/sites/default/files/anexos/5544-5536-1-PB.pdf>

CORREIA, J. Conde, “Prova Digital: as leis que temos e a lei que deveríamos ter”, *Revista do Ministério Público*, n.º 139 (2014)

CORREIA, J. Conde, “Artigo 179º”, *Comentário Judiciário do Código de Processo Penal*, Tomo II, 2ª Edição, Almedina, 2020

DIAS, J. Figueiredo, “O Novo Código de Processo Penal”, *Textos Jurídicos – I*, Ministério da Justiça, 1987

DIAS, J. Figueiredo, *Direito Processual Penal*, Coimbra Editora, Clássicos Jurídicos, reimpressão, 2004

DIAS, J. Figueiredo, “Sobre os sujeitos processuais no novo Código de Processo Penal”, *O Novo Código de Processo Penal. Jornadas de Direito Processual Penal*, Almedina, 1995

FIDALGO, Sónia, “A apreensão de correio eletrónico e a utilização noutro processo das mensagens apreendidas”, *Revista Portuguesa de Ciência Criminal*, n.º 1 (2019)

LEITE, A. Lamas, “As Escutas Telefónicas – Algumas reflexões em redor do seu regime e das consequências processuais derivadas da respetiva violação”, *Faculdade de Direito da Universidade do Porto*, 2004

LOPES, J. Mouraz, “Escutas Telefónicas: seis teses e uma conclusão”, *Revista do Ministério Público*, n.º 104 (2005)

MESQUITA, P. Dá, “Prolegómeno sobre prova eletrónica e interseção de telecomunicações no direito processual penal português e a Lei do Cibercrime”, *Processo Penal, Prova e Sistema Judiciário*, Wolters Kluwer/Coimbra Editora, 2010

MILHEIRO, T. Caiado, “Artigo 187º”, *Comentário Judiciário do Código de Processo Penal*, Tomo II, Almedina, 2019

- NEVES, R. Castanheira, *As ingerências nas comunicações eletrónicas em processo penal. Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*, Coimbra Editora, 2011
- NUNES, D. A. Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018
- RAMALHO, D. Silva, *Métodos ocultos de investigação criminal em ambiente digital*, Almedina, 2017
- RAMOS, A. Dias, *A prova Digital em Processo Penal: o correio eletrónico*, 2ª Edição atualizada e ampliada, Chiado Editora, 2017
- RAMOS, Vânia, “Âmbito e Extensão do Segredo das Telecomunicações”, *Revista do Ministério Público*, n.º 11 (2007)
- RODRIGUES, B. Silva, *Da Prova Penal, Bruscamente... As face(s) oculta(s) dos Métodos Ocultos de Investigação Criminal*, Rei dos Livros, 2010
- SILVA, G. Marques da, *Curso de Processo Penal*, Vol. II, 5ª Edição revista e atualizada, Verbo
- VALENTE, M. M. Guedes, *Escutas Telefónicas – Da Excepcionalidade à Vulgaridade*, 2ª Edição, Almedina
- VENÂNCIO, P. Dias, *Lei do Cibercrime, Anotada e Comentada*, Coimbra Editora, 2011
- VERDELHO, Pedro, “A nova Lei do Cibercrime”, *Scientia Iuridica*, Tomo LVII, n.º 320 (2009)
- VERDELHO, Pedro, “Apreensão de correio eletrónico em Processo Penal”, *Revista do Ministério Público*, n.º 100 (2004)
- VERDELHO, Pedro, “A obtenção de prova em ambiente digital”, *Revista do Ministério Público*, n.º 99 (2004)
- VERDELHO, Pedro, “A Convenção do Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa”, *Direito da Sociedade da Informação*, Vol. VI, Coimbra Editora, 2006