UNIVERSIDADE CATÓLICA PORTUGUESA

Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – Análise à luz do Acórdão do Supremo Tribunal de Justiça n.º 10/2023

Madalena Maria C. L. Fernandes

Dissertação com vista a obter o grau de Mestre em Direito na especialidade de Forense

Sob a orientação de:
Prof. Dr. Henrique Salinas

Faculdade de Direito | Escola de Lisboa
Março 2024

UNIVERSIDADE CATÓLICA PORTUGUESA

Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – Análise à luz do Acórdão do Supremo Tribunal de Justiça n.º 10/2023

Madalena Maria C. L. Fernandes

Dissertação com vista a obter o grau de Mestre em Direito na especialidade de Forense

Sob a orientação de:
Prof. Dr. Henrique Salinas

Faculdade de Direito | Escola de Lisboa
Março 2024

Agradecimentos

Primeiramente, ao meu orientador Professor Doutor Henrique Salinas, por toda a disponibilidade e compreensão ao longo deste percurso.

À minha mãe, o meu maior exemplo, não só pela incrível jurista que é, mas principalmente pela força, garra e dedicação que revela em todos os desafios que a vida apresenta. Motivas-me a ser melhor todos os dias.

Ao meu pai, por acreditar em mim mesmo quando eu não acredito.

A ambos pelo amor, pelos sacrifícios e pelas oportunidades que me têm vindo a proporcionar ao longo de toda a vida. Tudo o que sou e o que faço é graças a vocês.

Ao meu irmão, que tem sempre uma palavra de força.

Aos meus avôs, que vivem todas as minhas conquistas com a maior intensidade. Espero que estejam orgulhosos.

Às minhas amigas que iniciaram o percurso no mundo do Direito comigo e que estão do meu lado a cada passo. Mariana, Sara, Sofia e Beatriz, só vocês compreendem verdadeiramente o que significa concluir mais uma etapa.

À minha amiga e companheira Joana. Tenho a certeza que este é apenas o início de uma amizade que vai durar para toda a vida.

Ao António, pelo amor, pelo apoio, pelo carinho e por me aturar em todas as horas.

Modo de citar e outras convenções

A presente dissertação foi redigida em Língua Portuguesa, de acordo com o atual Acordo Ortográfico da Língua Portuguesa.

Todas as citações apresentadas referem-se a obras, jurisprudência e legislação consultadas, disponíveis online ou em formato físico.

As referências relativas a jurisprudência, ao longo do corpo da dissertação, serão redigidas de forma sucinta, referindo apenas o Tribunal decisor, a data do Acórdão e o relator. O número do processo constará na bibliografia.

As referências a legislação proveniente de entidades internacionais, ao longo do corpo da dissertação, serão redigidas de forma sucinta, indicando a denominação do diploma e a sua data de publicação. A referência completa, incluindo a hiperligação para a fonte consultada, constará na bibliografia.

As referências a iniciativas legislativas, ao longo do corpo da dissertação, serão redigidas de forma sucinta, indicando a denominação da iniciativa e a sua data de publicação. A referência completa constará na bibliografia.

As citações em notas de rodapé e as referências bibliográficas serão apresentadas de acordo com a 7.ª edição das normas APA (*American Psychological Association* – https://apastyle.apa.org/)

Em notas de rodapé, a citação de excertos de livros será apresentada em sistema autor-data. Far-se-á referência às páginas, sempre que possível. A referência completa constará na bibliografia.

Em notas de rodapé, a citação de artigos de revista será apresentada em sistema autor-data. Far-se-á referência às páginas, sempre que possível. A referência completa constará na bibliografia.

Em notas de rodapé, a citação de artigos consultados online será apresentada em sistema autor-data. Far-se-á referência às páginas, sempre que possível. A referência completa constará na bibliografia. A hiperligação para o sítio onde a obra se encontra disponível constará na bibliografia.

Na bibliografia final, cada obra ou artigo serão mencionados tendo em conta os elementos disponíveis, seguindo os seguintes critérios: O nome do autor deve vir indicado em forma invertida (apelido, nome); Deve identificar-se o autor, em maiúsculas pequenas, pelo último apelido, com a exceção dos autores espanhóis que devem ser indicados pelo penúltimo; Nos artigos publicados em revistas, em obra coletiva ou capítulo de livro deve indicar-se a primeira e última página do mesmo; Ao nome do autor deve seguir-se a data de publicação.

Na bibliografia final, os livros serão citados de acordo com a seguinte ordem: Apelido (em maiúsculas), nome do autor, data de edição, título da obra (em itálico), número de edição, editora e local de edição.

Na bibliografia final, os artigos de revistas serão citados de acordo com a seguinte ordem: Apelido (em maiúsculas), nome do autor, data de edição, título do artigo (entre aspas), título da revista (em itálico), número e/ou ano de publicação.

Em caso de artigos consultados online, constará, para além da identificação dos respetivos elementos, os endereços das páginas *web*.

Nas decisões jurisprudenciais portuguesas, será incluída na bibliografia final o tribunal, data, relator e respetiva fonte.

As abreviaturas encontram-se identificadas na lista de abreviaturas, por ordem alfabética.

No âmbito da primeira utilização dos termos abreviados para siglas, a sigla será mencionada após a denominação, entre parêntesis curvos.

Expressões em língua estrangeira serão apresentadas em itálico.

Transcrições de disposições legais, obras e jurisprudência serão destacadas entre aspas duplas.

O corpo da presente dissertação, incluindo notas de rodapé e excluindo espaços, tem um total de 90.000 caracteres.

Lista de abreviaturas

Ac. – Acórdão
Art. – Artigo
CPP – Código de Processo Penal
CRP ou Constituição – Constituição da República Portuguesa
JIC – Juiz de Instrução Criminal
LC ou Lei do Cibercrime – Lei n.º 109/2009
MP – Ministério Público
p. – Página
PJ – Polícia Judiciária
OPC – Órgãos de Polícia Criminal
SMS – *Short Message Service*
STJ – Supremo Tribunal de Justiça
TC – Tribunal Constitucional
TRC – Tribunal da Relação de Coimbra
TRE – Tribunal da Relação de Évora
TRG – Tribunal da Relação de Guimarães
TRL – Tribunal da Relação de Lisboa
TRP – Tribunal da Relação do Porto

Resumo

Num Acórdão recente, o Supremo Tribunal de Justiça declarou que, na fase de inquérito, compete ao juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente de se encontrarem abertas/lidas ou fechadas/não lidas, que se afigurem ser de grande interesse para descoberta da verdade ou para a prova, nos termos do artigo 17.º da Lei do Cibercrime.

Todavia, levanta-se a questão de determinar quais são as consequências práticas desta decisão jurisprudencial.

A dissertação em apreço versa sobre questões processuais inerentes ao regime da apreensão de correio eletrónico e comunicações semelhantes, com especial destaque para a problemática de uma eventual distinção entre e-mails abertos ou lidos e e-mails fechados ou não lidos, à luz do Acórdão do Supremo Tribunal de Justiça n.º 10/2023.

Palavras-chave: direito processual penal, prova, apreensão, e-mails e comunicações semelhantes

Abstract

In a recent ruling, the Supreme Court of Justice declared that, at the investigation stage, it is up to the preliminary judge to order or authorize the apprehension of electronic e-mails or other records of communications of a similar nature, regardless of whether they are open/read or closed/unread, which appear to be of great interest for the discovery of the truth or for evidence, under the terms of article 17 of the Cybercrime Law.

However, the question arises as to what the practical consequences of this case law decision are.

This dissertation deals with procedural issues inherent in the system for the capture of emails and similar communications, with particular emphasis on the problem of a possible distinction between open or read emails and closed or unread emails, in the light of Supreme Court Ruling n.º 10/2023.

Keywords: criminal procedure law, evidence, apprehension, e-mails and similar communications

Índice

1. Introdução

O fenómeno da globalização encontra-se indiscutivelmente associado ao desenvolvimento da tecnologia e a relevantes avanços informático-digitais. O Direito, enquanto regulador da sociedade, não fica indiferente às capacidades das ferramentas informáticas.

Contudo, nem tudo o que a Internet comporta é positivo, pois cada vez mais a criminalidade típica do mundo offline se transpõe para o ambiente digital.[1]

Desde logo, as novas formas de comunicação, nomeadamente através de meios informáticos, acabam por contribuir significativamente para o aparecimento de uma nova realidade criminal, conhecida como cibercrime.

Atualmente, os crimes de *phising*[2] e de *ransomware*[3] continuam a ser os mais comuns.

No entanto, a par destes fenómenos, cada vez mais se constata que outros ilícitos são cometidos online, por exemplo, através de troca de e-mails ou mensagens, enviadas através das redes sociais, utilizando um smartphone ou outro meio eletrónico como instrumento do crime.

Esta crescente onda de crimes digitais motivou a que o Direito, enquanto realidade em constante mutação, iniciasse a tão necessária adaptação a este novo contexto penal.

Para além das inúmeras questões de direito substantivo, o crime cometido no contexto digital levanta também problemas de índole processual, o que obrigou o legislador a procurar respostas para solucionar os desafios inerentes a esta nova realidade criminal.

O surgimento da prova digital e de legislação que a regulasse foi essencial para o início do combate à criminalidade informática[4].

No nosso ordenamento jurídico, a consagração da Lei n.º 109/2009[5], de 15 de setembro, conhecida como a Lei do Cibercrime, impulsionou um movimento de mudança no que diz respeito a esta matéria, procurando colmatar as dificuldades sentidas na nossa legislação.

Este instrumento legal criou medidas de cooperação internacional, alargou o leque da tipificação dos crimes informáticos, e veio inserir os chamados meios de obtenção de prova digital[6].

Um dos meios de obtenção de prova previstos na Lei do Cibercrime é a apreensão de correio eletrónico e registos de comunicações de natureza semelhante.

Cada vez mais se torna imprescindível a utilização de mensagens de correio eletrónico e de natureza semelhante, nas quais se inclui as mensagens enviadas por telemóvel ou nas redes sociais, como meio de prova no processo penal, através da sua apreensão em sistemas informáticos[7].

Porém, devido às suas características especiais, a obtenção deste meio de prova levanta inúmeras questões jurídicas.

Assim, esta dissertação tem como principal propósito a breve exposição e o esclarecimento de

---

[1] CARRAPIÇO (2005), p. 177

[2] Ato ilícito que consiste na recolha e utilização fraudulenta de credenciais de pagamento para substração devalores às vítimas.

[3] Ato ilícito que consiste na encriptação de dados informáticos para proceder a posteriores pedidos de resgate

[4] BRANCO (2021), p. 2

[5] Lei n.º 109/2009 de 15 de Setembro Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

[6] BRANCO (2021), p. 2

[7] BRANCO (2021), p. 19

dificuldades sentidas com a prova digital, no caso concreto das comunicações eletrónicas, e com a sua obtenção, com foco no Acórdão de Fixação de Jurisprudência n.º 10/2023[8] de 11.10.2023.

Pretende-se apontar alguns dos problemas decorrentes do regime previsto na Lei do Cibercrime e a sua compatibilização com o regime estipulado no Código de Processo Penal.

Por fim, considerando o Acórdão de Uniformização de Jurisprudência de 10.11.2023, destaca-se a relevância da problemática da potencial distinção entre e-mails abertos ou lidos e fechados ou não lidos.

Mais do que encontrar soluções absolutas e definitivas, procura-se expor as principais problemáticas inerentes a esta questão, de forma a compreender as decisões tomadas pelo legislador nesta matéria e os resultados práticos a que conduzem.

Para tal, procede-se a uma divisão da presente exposição em temáticas distintas, que se traduzem nos seguintes capítulos: breve contextualização da prova no sistema penal português; conceitos de prova e crime digital; definição dos serviços de correio eletrónico e dos meios de comunicação semelhantes; regras especiais de Lei do Cibercrime relativas à recolha de prova em suporte eletrónico: caso concreto de apreensão de correio eletrónico e registos de comunicações de natureza semelhante; necessidade de articulação da Lei do Cibercrime com as normas do Código de Processo Penal: algumas questões problemáticas; por fim, análise da problemática da potencial distinção entre e-mails abertos e fechados à luz do Acórdão do Supremo Tribunal de Justiça de 10.11.2023[9].

2. Breve contextualização da prova no sistema penal português

De forma a compreender melhor as características particulares deste tipo de prova, ao dar início a este estudo considerou-se importante aludir ao conceito de prova no processo penal português. Assim, no primeiro ponto desta discussão, concretiza-se a distinção entre prova, meios de prova e meios de obtenção de prova e, posteriormente, são referenciados os princípios que regulam a prova no sistema português mais relevantes para a temática em causa.

O processo penal português tem estrutura acusatória: quem investiga é uma entidade diferente da que julga[10].

Acresce que a investigação se apoia maioritariamente no instituto da prova. Assim, levanta-se a questão de definir em que consiste a prova.

Segundo Paulo de Sousa Mendes[11], podemos afirmar que, no processo penal, a prova é "o esforço metódico através do qual são demonstrados os factos relevantes para a existência do crime, a punibilidade do arguido e a determinação da pena ou medida de segurança aplicáveis".

Transpondo a necessidade de procurar definir conceitos técnico-doutrinais referentes a esta temática, é possível considerar que, de forma simplista, provar algo no contexto do Direito é produzir um estado de certeza no julgador, tão forte, que o leva a valorar determinada situação

[8] Acórdão do Supremo Tribunal de Justiça de 11.10.2023 (Pedro Branquinho Dias), in https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/9b1e715fa7cdbceb80258a4b003f6591?OpenDocument

[9] Acórdão do Supremo Tribunal de Justiça de 10.11.2023 (Pedro Branquinho Dias), in https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/10-2023-224081976

[10] BRANCO (2021), p. 10

[11] MENDES (2004), p. 132

como verdadeira[12], de forma a ser possível considerar que determinado facto ocorreu.

Considerando que a prova pretende demonstrar factos relevantes para a existência de um ilícito e justificar, consequentemente, a aplicação de uma pena, é importante mencionar que esses factos são demonstrados através de meios de prova.

Os meios de prova são fontes de convencimento legais que se distinguem da própria prova, uma vez que é através destes meios que o legislador se vai servir para gerar a real convicção sobre um determinado facto, introduzindo no procedimento pelo menos um elemento de prova.

Por outras palavras, os meios de prova caracterizam-se por ser o caminho a percorrer e a prova, strictu sensu, o destino ou resultado que se ambiciona[13].

A título de exemplo, perante um tipo de prova pessoal como a testemunhal, o meio de prova será o depoimento da testemunha.

Por outro lado, numa prova real que resulta da observação de coisas, como a prova documental, o meio de prova será o documento.

Questão distinta do conceito de prova e de meios de prova, são os meios de obtenção de prova.

Os meios de obtenção de prova correspondem aos instrumentos de que se servem as autoridades judiciárias para investigar e recolher meios de prova.

Tendo por base a metáfora previamente mencionada, se os meios de prova são o caminho a percorrer e a prova o destino, os meios de obtenção de prova serão o instrumento usado para percorrer esse caminho.

Importa ainda fazer uma breve menção ao artigo 125.º do Código de Processo Penal (CPP) que, sob epígrafe "legalidade da prova", estabelece que "são admissíveis as provas que não forem proibidas por lei".

No nosso ordenamento jurídico não há um elenco taxativo das provas admissíveis, consagrou-se a liberdade de prova desde que não constitua prova proibida por lei.

Encontra-se aqui consagrado um dos princípios mais relevantes em matéria probatória, o princípio da legalidade da prova.

Partindo desta premissa, cabe fazer uma breve referência a um tópico de indiscutível importância, as Provas Proibidas.

O ordenamento jurídico português, na Constituição da República Portuguesa (CRP ou Constituição) e no Código de Processo Penal, inclui determinadas proibições em matéria de prova.

No âmbito da Constituição da República Portuguesa, partindo dos artigos 24.º e 25.º, tanto a vida humana como a integridade física das pessoas são consideradas invioláveis. Neste sentido, o número 2 do artigo 25.º estabelece que "ninguém pode ser submetido a tortura, nem a tratos ou penas cruéis, degradantes ou desumanos.".

Já o número 8 do artigo 32.º da CRP especifica que "são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações"

Acresce que, perante a relevância no contexto desta dissertação, é ainda importante referenciar o número 1 do artigo 34.º da CRP, que estabelece que "o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.".

É de facto notória a preocupação do legislador no respeito pelos imperativos constitucionais atinentes à dignidade da pessoa humana, à integridade pessoal e à intimidade da vida privada e

[12] BRANCO (2021), p. 10
[13] FREITAS (2017), p. 12

familiar, próprios de um Estado de Direito Democrático.[14]

Quanto às provas proibidas no CPP, cabe destacar o entendimento de Francisco Marcolino de Jesus[15], que parte da distinção entre temas de prova proibidos, meios de prova proibidos e métodos proibidos de prova.

Os temas de prova proibidos, previstos no artigo 137.º do CPP, reportam aos temas que a lei não permite que sejam investigados, ou seja, parte da ideia de que determinados factos não podem ser objeto de prova.

Já os meios de prova proibidos correspondem aos meios de prova cuja valoração a lei não permite como tal, devido à falta de um qualquer requisito legal, o que resulta na indisponibilidade da sua utilização.

Por fim, os métodos proibidos de prova consistem em determinados procedimentos que não podem ser utilizados no contexto de recolha de prova, estando previstos nos números 1, 2 e 3 do artigo 126.º do CPP.

3. Conceitos de crime digital e prova digital

Ultrapassada esta questão considera-se imperativo procurar clarificar sucintamente em que consiste o crime e a prova digital.

A discussão sobre prova digital assume ainda mais importância ao constatar que ainda não existe uma definição consensual sobre o que consubstancia um crime digital.

Primeiramente cabe ressalvar que a regulação desta temática se encontra circunscrita a três diplomas: o Código de Processo Penal[16], a Lei n.º 32/2008[17], de 17 de Julho, referente à Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas, e a Lei n.º 109/2009, de 15 de Setembro, a que se dá o nome de Lei do Cibercrime.

No entanto, perante a necessidade de proceder a uma exposição breve sobre o tema, que não permite uma análise aprofundada sobre a temática em apreço, apenas será feita referência às estipulações previstas no Código de Processo Penal e na Lei do Cibercrime.

Em termos simplistas, o Professor David Silva Ramalho[18] define o crime digital como "o comportamento criminoso praticado em ambiente digital contra sistemas ou dados informáticos ou mediante o uso de sistemas informáticos e tecnologias de informação".

Neste sentido, releva ainda a distinção doutrinal entre os conceitos de cibercrime em sentido próprio e em sentido impróprio.

Enquanto no primeiro se incluem os crimes que "apenas podem ser praticados em formato digital e que incluirão quase todos os tipos legais previstos na Lei do Cibercrime", o segundo abarca "os crimes que apenas são praticados por esse via [digital], pese embora o pudessem ser por qualquer outra", como as ameaças ou injúrias praticas na internet.[19]

Deste modo, em sentido amplo, a criminalidade informática “englobará toda a panóplia de

[14] GONÇALVES e ALVES (2009), p.121

[15] JESUS (2015), pp. 92 – 104.

[16] Aprovado pelo Decreto-Lei n.º 78/1987, de 17 de fevereiro

[17] Lei n.º 32/2008 de 17 de Julho transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações

[18] RAMALHO (2017), p. 20 e ss

[19] MENDES e RAMALHO (2019)

atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais do que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios".[20]

Já em sentido estrito, apenas "abarcará aqueles crimes em que o elemento digital surge como parte integrador do tipo legal ou mesmo como seu objeto de proteção".[21]

Assim, conclui-se que o juízo relevante nesta matéria é o meio utilizado para a prática do crime.

Rita Coelho dos Santos[22], por outro lado, adianta uma classificação tripartida, nos termos da qual distingue: os crimes tipicamente informáticos, ou seja, aqueles que o legislador reconhece como crimes eminentemente ligados à informática, na medida em que o objeto ou instrumento da ação é tecnológica ou crimes potencialmente informáticos, não podendo o tipo ser preenchido se não se verificar qualquer ação sobre ou através desses equipamentos; os crimes essencialmente informáticos, que compreendem apenas aqueles em que o próprio bem jurídico ofendido consiste numa realidade de natureza informática com dignidade suficiente para merecer a tutela penal; e os crimes acidentalmente informáticos, isto é, aqueles em que a utilização do computador é apenas um novo modus operandi, não contendendo com o preenchimento do respetivo tipo legal.

Superada esta questão, importa determinar em que consiste a prova digital.

Segundo o Professor Paulo Sousa Mendes[23], prova digital corresponde à informação em formato digital, armazenada em repositório digital ou transmitida por sistemas informáticos que, de algum modo, possa contribuir para a explicação ou demonstração de um facto.

Já Benjamim Silva Rodrigues[24] define a prova digital "como qualquer tipo de informação, com valor probatório, armazenada [em repositório electrónico-digitais de armazenamento] ou transmitida [em sistemas e redes informáticas ou rede de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital".

Por outro lado, Armando Dias Ramos[25] considera que "a prova digital corresponde a toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta".

De referir que prova digital pode assumir várias formas, destacando, para o caso, os e-mails, ou as mensagens enviadas por telemóvel ou, ainda, através das redes sociais.

Independentemente da definição defendida, é possível identificar algumas características inerentes à prova digital[26]: trata-se de um tipo de prova incorpóreo, temporário, fungível e volátil.

No contexto da exposição em causa, cabe destacar a característica da incorporeidade.

Sendo que este tipo de prova se encontra num formato distinto, formato digital, não corresponde a um bem corpóreo.

Consequentemente, é indiscutível que a sua apreensão apresenta especial dificuldade, pois é constituída por meios técnicos específicos que exigem certos conhecimentos técnicos especializados para a apreender e disponibilizar.

---

[20] VENÂNCIO (2011), p. 17
[21] VENÂNCIO (2011), p. 17
[22] SANTOS (2005), p. 32 ss
[23] MENDES e RAMALHO (2019)
[24] RODRIGUES (2011), p.39
[25] RAMOS (2014), p. 86
[26] RAMOS (2014, p. 88; MESQUITA (2011), pp.100-110

Acresce que a prova digital necessita de ser manuseada de forma particularmente cuidadosa perante a forte possibilidade de ser alterada, ocultada ou até mesmo eliminada, quer seja pelo decurso do tempo, quer seja por intervenções de terceiro.
Assim, perante as especificidades inerentes à prova digital, levanta-se a questão de determinar qual o regime aplicável à obtenção de provas como emails, mensagens enviadas pelo WhatsApp ou pelo Facebook.

4. Os serviços de correio eletrónico e de comunicações semelhantes como meios de prova

Para que nos possamos aproximar da questão essencial, é imperativo proceder a uma análise dos serviços de correio eletrónico e dos meios de comunicação semelhantes enquanto meios de prova.
De acordo com a definição dada pelo legislador europeu, nos termos do artigo 2.º alínea h) da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho[27], o "correio eletrónico é qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário a recolher.".
Nos termos do ordenamento jurídico português, este conceito encontra-se previsto na alínea b) do número 1 do artigo 2.º da Lei n.º 41/2004[28], instrumento jurídico que transpôs para a ordem jurídica nacional a referida Diretiva.
Benjamim Silva Rodrigues[29] define o correio electrónico como "qualquer mensagem textual, vocal, sonora ou gráfica, combinada ou não, enviada através de um terminal de um ponto de uma rede pública de comunicações electrónicas para outro terminal conexionado a tal rede, podendo ser, temporária ou definitivamente, armazenada na rede ou equipamento terminal do destinatário até que o mesmo proceda à sua recolha, mediante 'carregamento' e correspectivo 'descarregamento' em equipamento informático que torna a mensagem humanamente perceptível (ou lisível) pelos vários sentidos (visão ou audição)".
Já na esfera de Armando Dias Ramos[30], correio eletrónico corresponde a "um programa informático que permite a comunicação instantânea, de modo diferido, entre quem a envia e quem a recebe, através das redes de informação e comunicação, independentemente do local em que estes se encontrem, sem a necessidade deste se encontrar instalado no computador".
Quanto às comunicações semelhantes, segundo Rui Cardoso[31], é possível distinguir dois grupos: as comunicações realizadas pelo número de telefone, onde podemos inserir as SMS ou MMS; e as realizadas através da internet, que englobam programas de mensagens instantâneas, como por exemplo *Messenger*, *WhatsApp*, *Telegram*, *Discord*.
Tratando-se de ferramentas que permitem facilitar a comunicação, a verdade é que também acarretam inúmeros desafios, principalmente se considerados enquanto meios de prova.

[27] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)
[28] Lei n.º 41/2004 transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas
[29] RODRIGUES (2009), p. 572
[30] RAMOS (2014), p. 28
[31] CARDOSO (2018), p. 179

Efetivamente, aceder a esta informação pode consubstanciar uma forte violação de direitos constitucionalmente estabelecidos, nomeadamente o direito à inviolabilidade do domicílio e o sigilo da correspondência e de outros meios de comunicação privada e o direito à reserva da vida privada, como será devidamente demonstrado no próximo capítulo da presente dissertação.

Consequentemente, levantam-se inúmeras questões relativas à sua admissibilidade.

De forma a compreender qual a posição jurisprudencial maioritária no que respeita à admissibilidade destes meios probatórios, surge a necessidade de proceder a uma breve análise de alguns exemplos da jurisprudência portuguesa.

In casu, destaca-se o Acórdão do Tribunal da Relação de Évora de 09.01.2018[32], o Acórdão do Tribunal Relação Porto de 08.06.2018[33] e o acórdão do Tribunal da Relação do Porto de 20.01.2016[34].

Relativamente ao acórdão do Tribunal da Relação de Évora, processo 263/15.7T9ALR.E1, a arguida foi acusada da prática de um crime de injúria por um presidente de uma associação desportiva rival, perante o envio de e-mails insultuosos para o assistente com conhecimento de terceiros.

O Tribunal decidiu absolver a arguida do crime de que vinha acusada, tendo desconsiderado os e-mails por considerar não serem bastantes para fazer prova razoável do crime de injúria.

Porém, inconformado com a decisão, o assistente recorreu para o Tribunal da Relação.

O Tribunal deu provimento ao recurso, considerando que os e-mails, desde que apreendidos legalmente, constituem meio de prova mais do que suficiente para efetivamente provar a existência de um crime de injúria.

Relativamente ao acórdão do Tribunal da Relação do Porto, processo 293/20.7PAVFR.P1, reporta-se à acusação do arguido pela prática de um crime de violência doméstica e de um crime de injúria pela sua esposa.

O Tribunal decidiu absolver o arguido dos crimes de que vinha acusado, tendo para o efeito valorado as mensagens que o arguido trocara com a esposa via WhatsApp e das quais resultara que, afinal, mantinham um bom relacionamento apesar de estarem separados.

Inconformada com essa decisão e com a valorização dessas mensagens, a mulher recorreu para o Tribunal da Relação.

O Tribunal negou provimento ao recurso, confirmando o acórdão recorrido, ao decidir que as mensagens, vídeos, fotos e áudios trocados livremente via WhatsApp não estão protegidos pelos direitos constitucionais de reserva da intimidade da vida privada e da confidencialidade da mensagem pessoal, valendo como prova em processo penal.

Por fim, relativamente ao Tribunal da Relação do Porto, processo 1145/08.4PBMTS.P, o arguido, após ver prescindidos os seus serviços, numa tentativa de intimidação, procedeu ao envio de SMS injuriosos e ameaçadores aos representantes da sua antiga entidade patronal.

O arguido alega que a apresentação destas mensagens enquanto meio de prova consubstancia uma

---

[32] Acórdão do Tribunal da Relação de Evóra de 09.01.2018 (Alberto Borges), in http://www.dgsi.pt/jtre.nsf/-/8521E0E81EFC0B308025822700320074.

[33] Acórdão do Tribunal da Relação do Porto de 08.06.2022 (José António Rodrigues da Cunha), in https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/91a806c80947fbfa802588680048e9e3?OpenDocument

[34] Acórdão do Tribunal da Relação do Porto de 20.01.2016 (Artur Oliveira), in https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/54a82f139588437f80257f5a0033e764?OpenDocument

violação da sua vida privada.

Porém, o Tribunal acabou por considerar que se o arguido enviou ao ofendido uma mensagem por SMS, o seu destinatário pode fazer da missiva o uso que entender, nomeadamente apresentá-la às autoridades judiciárias para poder servir como prova de um crime de que é vitima.

O que a lei pretende tutelar é a intromissão na correspondência, na vida privada, no domicílio ou nas telecomunicações feitas sem o consentimento do respetivo titular (artigos 174.º, 176.º, 177.º e 187.º, do CPP).

Porém, esse nunca seria o caso dos autos, sendo que é o próprio titular da mensagem que a apresenta às autoridades para poder servir como prova de um crime de que é vítima.

Em suma, é possível concluir que o ordenamento jurídico português efetivamente assume que as mensagens de correio eletrónico, entre outras comunicações, podem ser usadas como meio de prova, reconhecendo a sua importância como fontes de material probatório.

5. Direitos fundamentais potencialmente restringidos com a apreensão de correio eletrónico e comunicações semelhantes

Segundo Figueiredo Dias, é possível identificar quatro finalidades inerentes ao processo penal: a realização da justiça, a descoberta da verdade material, a proteção dos direitos fundamentais e o estabelecimento da paz jurídica violada com a prática do crime.[35]

No âmbito da investigação, imprescindível para a descoberta da verdade material e, consequentemente, para a realização da justiça e o restabelecimento da paz jurídica, o Estado é, muitas vezes, obrigado a restringir os direitos fundamentais dos cidadãos.

Na opinião do autor, o processo penal visa "encontrar a solução justa e adequada para o caso concreto, no contexto de um sistema"[36].

Por outras palavras, surge a necessidade de procurar "a solução do conflito entre as exigências comunitárias e a liberdade de realização da personalidade individual"[37], na medida em que se verifica uma constante tentativa de contrabalançar por um lado os Direitos Fundamentais e o Direito Penal, que visam tutelar e proteger os bens jurídicos essenciais, e o Processo Penal que, frequentemente, viola os respetivos bens jurídicos em causa, sempre com o intuito de atingir as suas finalidades e, em última instância, garantir a eficácia do Direito e a proteção dos bens jurídicos.

Efetivamente, "os fundamentos do direito processual penal são, simultaneamente, os alicerces constitucionais do Estado; a concreta regulamentação de singulares problemas processuais deve ser conformada jurídico-constitucionalmente"[38].

A apreensão de mensagens de correio eletrónico e de comunicações similares enquanto meio de obtenção de prova é efetivamente justificada pela descoberta da verdade material.

No entanto, é incontestável o caráter intrusivo e lesivo desta atuação, uma vez que possibilita o acesso irrestrito a informações de caráter pessoal, ou seja, o acesso a informações da vida do indivíduo cujas mensagens foram apreendidas. O ato de apreensão de mensagens de correio eletrónico configura, indiscutivelmente, uma ingerência na correspondência privada o que pode

[35] DIAS (2004), p. 11 e ss
[36] DIAS (1991), p. 20
[37] DIAS (2004), p. 59
[38] DIAS (1974), p. 74. e ss.

resultar numa colisão com vários direitos e princípios fundamentais do Estado de direito democrático.[39]

Consequentemente, esta método de obtenção de prova levanta inúmeras questões relativas à necessidade de proteção de certos direitos fundamentais que podem ser colocados em risco mediante a apreensão.

De facto, exige-se uma ponderação e um equilíbrio entre a intervenção nas comunicações e a investigação criminal, de forma que os direitos fundamentais não sejam excessivamente sacrificados, devendo a restrição de qualquer direito se limitar ao estritamente imprescindível para a prossecução do interesse público.

Neste sentido, para que seja legítimo proceder à restrição de um direito fundamental, exige-se a verificação de inúmeros requisitos.

A restrição de qualquer direito só deve ser tolerada quando devidamente fundamentada, justificada e adequada ao caso concreto.

O número 2 do artigo 18.º da Constituição da República Portuguesa determina que a lei só pode proceder à restrição de direitos nos casos expressamente previstos constitucionalmente, ou seja, quando uma norma constitucional consagradora de um direito procede a uma remissão legal que não se limite conformação do direito.

Contudo, encontra-se hoje assente, na doutrina[40] e jurisprudência portuguesa, a admissibilidade de restrições legais implícitas em caso de colisão entre direitos ou entre estes e interesses constitucionalmente protegidos.

Neste sentido, o mesmo número 2 do artigo 18.º da Constituição da República Portuguesa condiciona a restrição de direitos liberdades e garantias constitucionais ao princípio da proporcionalidade, o que significa que a admissibilidade da afetação desfavorável de um direito depende da circunstância de essa restrição ser necessária e adequada à salvaguarda de outro direito fundamental ou de um interesse público constitucionalmente protegido dotados de maior peso ou relevância no contexto concreto em que opera a referida restrição.

Como refere Francisco Marcolino de Jesus[41], "o princípio de proporcionalidade ou proibição de excesso desdobra-se em três sub-princípios: 1) O princípio da conformidade ou adequação, que "impõe que a medida adotada para a realização do interesse público deve ser apropriada à prossecução do fim ou fins a eles subjacentes", isto é, "as medidas restritivas de direitos, liberdades e garantias devem revelar-se como um meio para a prossecução dos fins visados, com salvaguarda de outros direitos ou bens constitucionalmente protegidos"; 2) O princípio da exigibilidade ou da necessidade, "também conhecido como "princípio da necessidade" ou da "menor ingerência possível", segundo o qual, "As medidas restritivas têm de ser exigidas para alcançar os fins em vista, por o legislador não dispor de outros meios menos restritivos para alcançar o mesmo desiderato"; 3) O princípio da proporcionalidade em sentido restrito, "entendido como princípio da "justa medida" ou "proporcionalidade em sentido estrito (não poderão adotar-se medidas excessivas, desproporcionadas para alcançar os fins pretendidos)".

De forma a conciliar as finalidades conflitantes, o legislador estabeleceu critérios para a apreensão, exigindo a observância rigorosa desses pressupostos.

Todavia, é crucial reconhecer que a mobilização deste método de obtenção de prova pode resultar numa limitação significativa dos direitos, liberdades e garantias dos cidadãos.

---

[39] ROSA e CASANOVA (2021), p. 111
[40] NOVAIS (2010), p. 234
[41] JESUS (2015), p. 40 e ss

Dessa forma, torna-se imprescindível analisar detalhadamente os direitos que são restringidos, de forma a garantir que qualquer restrição é de facto proporcional e estritamente necessária para atingir os objetivos ambicionados, designadamente a descoberta da verdade material, a realização da justiça e o restabelecimento da paz jurídica.

5.1. Direito à reserva da intimidade da vida privada e familiar (artigo 26.º n.º 1 e 2 da CRP)

O direito à reserva sobre a intimidade da vida privada e familiar está consagrado no elenco de direitos, liberdades e garantias da Constituição da República Portuguesa, no número 1 do artigo 26.º, constituindo um direito de personalidade estritamente ligado ao princípio da dignidade da pessoa humana, que se traduz na simples qualidade de ser humano, independente de qualquer outra condição, na medida em que a dignidade da pessoa pressupõe que esta beneficie de um espaço de privacidade.[42]

Segundo Conde Correia, a "vida privada compreende aqueles factos, atitudes ou opiniões individuais e particulares, que não tenham qualquer relação com a vida pública e que possam, em determinado momento histórico, ser razoavelmente considerados confidenciais, por forma a impedir ou restringir a sua divulgação"[43]

Citando Rodrigues Bastos[44], inclui "todos aqueles atos que, não sendo secretos em si mesmos, devem subtrair-se à curiosidade pública por naturais razões de resguardo e melindre (…), em suma: sentimentos, ações e abstenções que podem ser altamente meritórios do ponto de vista da pessoa a que se referem, mas, que vistos do exterior, tendem a apoucar a ideia que delas faz o público em geral.".

Acresce que, inerente ao direito à reserva da intimidade da vida privada é possível delimitar dois direitos subjacentes: o direito de impedir o acesso de terceiros ou estranhos a informações sobre a vida privada e familiar e o direito a que ninguém divulgue as informações que tenha sobre a vida privada de outrem, traduzindo-se numa verdadeira proibição de ingerência na vida particular por terceiros, quer por acesso, quer por divulgação de informação, como consagrado no artigo 80.º do Código Civil.[45]

De facto, este direito "compreende, em qualquer caso, não somente o direito de oposição à divulgação da vida privada (*public disclosure of private facts*), mas também o direito ao respeito da vida privada, ou seja, o direito de oposição à investigação sobre a vida privada (*intrusion*)"[46]

Naturalmente, o direito à reserva da intimidade da vida privada é um direito fortemente afetado perante a autorização de uma investigação no âmbito de um processo de natureza criminal.

In casu, a apreensão de mensagens de correio eletrónico e de comunicações semelhantes pode resultar numa violação direta do direito à reserva da intimidade da vida privada e familiar, ao expor detalhes íntimos da vida das pessoas, revelar segredos pessoais, comprometer relacionamentos familiares ou profissionais e até mesmo colocar em risco a segurança dos indivíduos.

Permite-se a ingerência na vida privada dos sujeitos, sendo que a sua intimidade acaba por ser exposta, com a agravante do eventual desconhecimento dessa ingerência.

---

[42] VASCONCELOS (2006), p. 63
[43] CORREIA (1999), p. 49
[44] BASTOS, R., cit por DRAY (2008), p. 55
[45] CANOTILHO e MOREIRA (2007), p. 181
[46] MIRANDA e MEDEIROS (2010), p. 620

5.2. Direito à inviolabilidade de meios de comunicação privada, da correspondência e das telecomunicações (artigo 34, n.º 1 e 4 CRP)

Nos termos dos números 1 e 4 da Constituição da República Portuguesa, "o domicílio sigilo da correspondência e dos outros meios de comunicação privada são invioláveis", sendo "proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo penal".

A inviolabilidade da correspondência e de outros meios de comunicação está relacionada com a reserva da intimidade da vida privada prevista no artigo 26.º da Constituição.

Efetivamente, o direito a intimidade da vida privada atua enquanto garante de proteção de reserva e de resguardo, pressupondo a faculdade de impedir a revelação de factos relacionados com a vida íntima e familiar do sujeito.

Segundo Conde Correia, o "direito ao sigilo da correspondência e de outros meios de comunicação privada protege toda a espécie de comunicação interpessoal, privada ou não, efetuada por intermédio da correspondência e das telecomunicações, independentemente do meio técnico utilizado ou do seu conteúdo"[47].

O Tribunal Constitucional, no âmbito do Acórdão n.º 687/2021[48], com referência a jurisprudência anterior[49] sobre o direito fundamental à inviolabilidade da correspondência e das comunicações, considerou que "o artigo 34.º da Constituição tem por propósito consagrar e proteger o direito fundamental à inviolabilidade do domicílio e da correspondência, ou seja, e prima facie, a liberdade de manter uma esfera de privacidade e sigilo, livre de interferência e ingerência estadual, quer no que respeita ao domicílio, quer — sendo esta a dimensão relevante para o caso *sub iudice* — quanto à comunicação. É, aliás, entendimento doutrinal sedimentado que o âmbito de proteção da norma constitucional abrange todos os meios de comunicação individual e privada, e toda a espécie de correspondência entre pessoas, em suporte físico ou eletrónico, incluindo não apenas o conteúdo da correspondência, mas o tráfego como tal (espécie, hora, duração, intensidade de utilização), excluindo-se apenas a categoria residual de dados pessoais, isolados de qualquer processo de comunicação, efetivo ou tentado."

Todavia, a abertura constitucional do número 4 do artigo 34.º n.º 4 da Constituição da República Portuguesa permitiu a criação de tipos de ingerência nas comunicações: "i) a ingerência nas comunicações postais e telegráficas, rectius, correspondência – comunicação escrita; ii) a ingerência nas comunicações telefónicas – comunicações orais"; "a ingerência nas comunicações não telefónicas mas a elas equiparadas – correio eletrónico, comunicações telemáticas e outras; iv) a ingerência nas comunicações entre presentes – captação em ambiente físico, fora das redes de comunicações eletrónicas".[50]

Assim, só no domínio do processo penal é que aquela lei ordinária pode prever restrições esta garantia. As finalidades inerentes ao processo penal, designadamente à procura da verdade material, pressupõem obtenção de provas que permitam validar e legitimar essa mesma verdade.

Em consequência, justifica-se a restrição a este direito à comunicação reservada, desde que esta

[47] CORREIA (1999), p. 51

[48] Acórdão do Tribunal Constitucional n.º 687/2021 de 22.09.2021, in https://diariodarepublica.pt/dr/detalhe/acordao-tribunal-constitucional/687-2021-171674458

[49] Designadamente Acórdão do Tribunal Constitucional n.º 464/2019 de 21.10.2019, in https://www.tribunalconstitucional.pt/tc/acordaos/20190464.html

[50] RODRIGUES (2011), p. 127

restrição seja devidamente avaliada em termos de necessidade, adequação e proporcionalidade.

5.3 Direito à palavra (artigo 26.º n.º 1 CRP)

Nos termos do número 1 do artigo 26.º da Constituição, confere-se proteção constitucional à palavra.

Cabe referir que este preceito remete para a proteção da palavra falada, visto que a "fala é a expressão superior, em termos antropológicos, de uma qualquer relação comunicacional, já que pelo falar se consegue, de maneira comprimida, transmitir, em um espaço de tempo breve, uma quantidade de fluxo informacional, certa e precisa, que outras formas comunicacionais se mostram incapazes de realizar"[51].

Neste sentido, "o direito à palavra desdobra-se, assim, em três direitos: (a) direito à voz, como atributo de personalidade, sendo ilícito, sem consentimento da pessoa, registar e divulgar a sua voz (com ressalva, é claro, do lugar em que ela foi utilizada); (b) direito às "palavras ditas", que pretende garantir a autenticidade e o rigor da reprodução dos termos, expressões, metáforas escritas e ditas por uma pessoa; (c) direito ao auditório, ou seja, a decidir o círculo de pessoas a quem é transmitida a palavra. Mais uma vez, este direito sofre de compressões no caso dos discursos públicos de agentes públicos e políticos."[52]

No âmbito da presente dissertação, apresenta especial relevância a discussão da dicotomia entre palavra falada e a palavra escrita, designadamente a necessidade de uma proteção acrescida da palavra falada.

De facto, no contexto de uma conversa falada, seja esta presencial ou telefónica, que ocorra em tempo real, "a palavra falada é proferida naquele momento, com o já mencionado sentido de vaporização"[53].

Trata-se de uma forma de comunicação que se pauta pela espontaneidade, não se verificando por parte do emissor da mensagem falada qualquer intenção ou perceção de uma eventual perpetuação da informação. A palavra falada caracteriza-se precisamente pelo seu caráter espontâneo, efémero e volátil, criando a expectativa de que o conteúdo da comunicação não será passível de ser reproduzido em momento posterior visto que desvanece imediatamente.[54]

Consequentemente, surge a necessidade de "impedir que aquilo que se pretendeu que fosse apenas uma expressão fugaz e transitória da vida se converta num produto registado e suscetível de ser utilizado a todo o tempo"[55]. Pressupõe-se que a palavra falada se vai extinguir no exato momento em que é proferida, esgotando o seu âmbito após o término da comunicação.

Por outro lado, a palavra escrita implica um maior grau de ponderação e reflexão, na medida em que o emissor da mesma se encontra consciente de uma eventual perpetuação do conteúdo perante a sua inserção num suporte físico que é independente do autor.

Esta diferenciação de conceitos traduz-se, evidentemente, numa distinta graduação ao nível de proteção constitucional.

Enquanto na palavra escrita o emissor tem consciência que o conteúdo pode efetivamente permanecer registada e no poder do destinatário, na palavra falada foi imperativo impor ao

[51] COSTA (1999), p. 50
[52] CANOTILHO e MOREIRA (2007), p. 467
[53] NEVES (2011), p. 178
[54] NEVES (2011), p. 48
[55] ANDRADE (2006), p. 245

destinatário da palavra a ilicitude do seu registo não autorizado de modo a proteger o emissor.

Consequentemente, enquanto a tutela da palavra falada remete para o número 1 do artigo 26.º da Constituição[56], a palavra escrita encontra proteção constitucional nos termos do número 4 do artigo 34.º[57] e do número 4 do artigo 35.º[58] do mesmo instrumento jurídico.

Acresce que, no âmbito do desenvolvimento das novas tecnológicas de informação, surgiu uma nova palavra: a palavra virtual.

De acordo com Faria Costa, "informática, mas sobretudo a informatização em rede, veio trazer a possibilidade de a palavra não ser escrita, nem falada, estar virtualmente visível em um ecrã por força de um jogo complexo cingido à simples lógica binária. O que permite a possibilidade de a palavra estar e não estar e, todavia, se se quiser, estando ou não estando, trazê-la ao mundo normal da palavra escrita em suporte de papel"[59].

Surge a necessidade de determinar para que regime deve remeter este novo meio de exercício da palavra, mais concretamente no âmbito do correio eletrónico e comunicações semelhantes.

Segundo Rita Castanheiro Neves, a "palavra registada com o propósito de ser enviada por correio eletrónico leva já em si o mesmo grau de ponderação que conferimos à palavra escrita, enquanto ato perpetuador de uma especifica mensagem que se sabe que permanecerá para além do ato em que chega ao destinatário da comunicação"[60].

Por outro lado, é imperativo refletir sobre uma eventual equiparação das mensagens instantâneas à palavra falada, na medida em que esta troca de mensagens corresponde igualmente a um meio de expressão irrefletido e espontâneo, que possivelmente careça de proteção acrescida.

Ainda mais complexa é a possibilidade de proceder ao envio de uma mensagem de voz, por meio de um *smartphone*, mediante a utilização de uma aplicação de mensagens instantâneas.

Todavia, apesar da sua inquestionável pertinência, estas questões ainda não foram devidamente respondidas quer pela jurisprudência, quer pela doutrina.

6. Breve análise da evolução da regulamentação da apreensão de correio eletrónico no ordenamento jurídico português

De modo a compreender devidamente as complexidades deste meio de obtenção de prova, é imperativo proceder a uma breve análise da evolução legislativa inerente à apreensão de correio eletrónico e meios de comunicação semelhante.

Até à entrada em vigor da Lei do Cibercrime não existiam no ordenamento jurídico português regras especiais concernentes à recolha de prova digital, ou seja, à prova em suporte eletrónico.

Consequentemente, a investigação dos crimes relacionados com a informática ocorria mediante a aplicação das previsões gerais do Código de Processo Penal, através de uma interpretação analógica.

O Código de Processo Penal divide os meios de obtenção da prova entre: exames, previstos nos artigos 171.° a 173.º, as revistas e buscas, previstas no artigos 174.° a 177.°, apreensão, prevista

[56] "A todos são reconhecidos os direitos (…) à palavra (…)"

[57] "É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal"

[58] "É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei"

[59] COSTA (1999), p. 56

[60] NEVES (2011), p. 48

nos artigo 178.° a 186.º e escutas telefónicas, previstas nos artigos 187.° e seguintes.

Porém, os meios de obtenção de prova previstos no Código de Processo Penal foram estritamente pensados pelo legislador para obtenção de provas corpóreas.

Levanta-se então a questão determinar como seria regulada a apreensão de correio eletrónico previamente à entrada em vigor da Lei do Cibercrime.

Até à entrada em vigor das alterações introduzidas no Código de Processo Penal em 2007, pela Lei n.º 48/2007[61], de 29 de Agosto, perante a ausência de regulamentação específica em matéria de apreensão de correio eletrónico, a doutrina e a jurisprudência maioritária defendiam a equiparação do correio eletrónico ao correio tradicional.[62]

Porém, na sistematização Código de Processo Penal de 1987, o legislador, no artigo 190.º, consagrou uma extensão da aplicação do regime das escutas "(…) às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone".

Inevitavelmente, surgiram as primeiras incertezas interpretativas, resultando em dúvidas relativamente à extensão do âmbito de aplicação deste preceito a meios de comunicação que operassem por meio da Internet.

No entanto, segundo Faria Costa, "ninguém dúvida de que todo o regime das escutas telefónicas tem de ser entendido como verdadeiramente excepcional. De sorte que já a norma de extensão, em um horizonte crítico muito rigoroso, não se compreende de maneira satisfatória. Ou seja: o regime excepcional, porque excepcional, não pode alargar-se, sob pena de contradição palmar e insanável. No entanto, o legislador alargou-o. Que razoável e não contraditória razão de ser se pode, então, encontrar para um tal alargamento? Só uma resposta pode caber à pergunta anterior: o legislador quis que os novos meios de telecomunicação da palavra fossem também susceptíveis de sobre eles se escutar, nas condições legais previstas, as conversações ou comunicações, mas o legislador não quis nem podia - porque se o fizesse cairia na insuportável contradição ou aporia normativa - que outros instrumentos de telecomunicação que possibilitam outro tipo de palavra, que não a falada, caíssem no âmbito das escutas telefónicas. Julgamos ser esta a interpretação mais correcta perante o carácter excepcional da norma que se estuda. O que, bom é de ver, não impede que o legislador - em diferente e autónoma valoração - possa, através de nova intervenção legislativa, vir a considerar que o conteúdo das comunicações levadas a cabo por meio da palavra virtual possa ser, legitimamente, apreendido. Mas para que isso aconteça deve antes haver norma que o permita. E isso é tarefa do legislador e não do intérprete"[63].

No mesmo sentido, Costa Andrade considerou que estaríamos perante "um regime em princípio reservado às formas de comunicação oral, isto é, que possibilitam a emissão e recepção da própria palavra falada. Dele estarão, por exemplo, excluídas formas de comunicação como o telégrafo ou o telefax. Será, assim, desde logo, por razões atinentes à carência de tutela. Isto por ser manifesto que a intromissão indevida nas comunicações telegráficas não actualiza o atentado ao direito à palavra, que constitui um dos coeficientes de maior peso da danosidade social das escutas telefónicas. Acresce ser a própria lei a submeter expressamente o telegrama ao regime específico - e diferente do das escutas telefónicas - da apreensão de correspondência. Este é, de resto, o entendimento prevalecente na Alemanha, apesar de os preceitos homólogos da StPO (§§100a) e

[61] Lei n.º 48/2007 que procede à alteração do Código de Processo Penal
[62] NUNES (a) (2018), p. 23
[63] COSTA (1999), p. 76-77

100b)) se reportarem não às escutas telefónicas, mas antes e de forma mais genérica às intromissões nas telecomunicações (Überwachung dês Fermeldeverkehrs)"[64].

De facto, conclui-se que a doutrina defendia a estrita aplicação do artigo 190.º a comunicações por via oral.

Todavia, no âmbito da Lei n.º 58/98[65], de 25 de Agosto, que alterou o Código de Processo Penal, o referido artigo 190.º sofreu alterações, numa tentativa de colmatar as dúvidas interpretativas suscitadas na redação originária do preceito, passando a consagra que "O disposto nos artigos 187.º, 188.º e 189.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, bem como à intercepção das comunicações entre presentes".

Verificou-se, pela primeira vez, a regulação específica da apreensão de mensagens de correio eletrónico enquanto meio de obtenção de prova.

Contudo, com a alteração ao Código de Processo Penal por via da reforma de 2007[66], o regime das escutas telefónicas sofreu alterações substanciais.

Cabe destacar, perante a sua importância indiscutível, o alargamento do âmbito de ampliação do artigo 190.º (atual 189.º), que permitiu a aplicação deste regime às comunicações ou conversações eletrónicas armazenadas em suporte digital.

Com a ampliação deste preceito, o legislador consagrou a possibilidade de intercetar as mensagens de correio eletrónico, ainda que constassem de suporte digital.

Esta opção legislativa foi alvo de fortes críticas na doutrina e jurisprudência portuguesa.

Efetivamente, o legislador desperdiçou uma oportunidade de regular, de modo autónomo e específico, a prova digital, optando por remeter este meio de prova tão particular para um regime que em pouco ou nada responde às características específicas da prova em suporte eletrónico.

Figueiredo Dias[67] descreveu a reforma enquanto uma oportunidade perdida, cujo desmérito se deveu às profundas lacunas legais relativamente aos institutos probatórios inerentes às novas tecnologias.

No mesmo sentido, Costa Andrade[68] evidencia a dificuldade de aplicação e controlo do direito por parte das instâncias legais, perante a consagração de uma cláusula de extensão que aplica o mesmo regime a três realidades distintas: intromissão nas telecomunicações; acesso a "documentos" guardados no computador e que resultaram de comunicações eletrónicas; gravações de conversas entre presentes.

Apesar da intenção do legislador de regular a apreensão de correio eletrónico, já recebido e armazenado, a realidade é que a aplicação do regime das escutas telefónicas se revela inadequada.

Primeiramente, dada a natureza do processo comunicacional e seu desfasamento temporal, não é possível considerar que, no âmbito de uma troca e mensagens de correio eletrónico, se esteja perante uma comunicação a ocorrer em tempo real.

Ademais, uma comunicação é, por conceito, uma realidade dinâmica, um processo comunicacional

---

[64] ANDRADE (2006), p. 274-275

[65] Lei n.º 58/98 que procede à alteração do Código de Processo Penal

[66] Lei n.º 48/2007 que procede à alteração do Código de Processo Penal

[67] DIAS (2008), p. 385

[68] ANDRADE (2009) (a), p. 185

que tem início no recetor e termina no emissor.[69]

Por outro lado, as mensagens de correio eletrónico são registos de uma comunicação, passíveis de serem armazenados e guardados.

Esta questão apresenta especial relevância uma vez que que enquanto nas conversações telefónicas o conteúdo é instantaneamente "eliminado", tratando-se de uma mensagem de correio eletrónico é possível aceder ao conteúdo comunicacional posteriormente.

Simultaneamente, ao remeter para o mesmo regime realidades comunicacionais distintas, o legislador não considerou que o nível de proteção constitucional exigível é distinto no caso das comunicações eletrónicas.

Enquanto no caso da palavra escrita o emissário tem plena consciência de que o destinatário adquire posse e controlo sobre a sua mensagem, permanecendo no espaço que é a Internet, a palavra falada extingue-se automaticamente, só podendo ser registada, de modo não autorizado, ilicitamente.

Consequentemente, justifica-se a tutela diferenciada destes processos comunicacionais, na medida em que sofrem ingerências distintas. De acordo com Benjamim Silva Rodrigues[70], apenas a palavra escrita carece de uma proteção a nível do direito à privacidade e à autodeterminação informacional.

Por fim, com a entrada em vigor da Lei do Cibercrime, o legislador efetivamente optou por abandonar a equiparação da apreensão do correio eletrónico às escutas telefónicas.

O legislador, no artigo 17.º da Lei do Cibercrime, consagrou um regime específico para a apreensão do correio eletrónico e comunicações semelhantes.

7. Regras especiais da Lei do Cibercrime relativas à recolha de prova em suporte eletrónico: caso concreto de apreensão de correio eletrónico e registos de comunicações de natureza semelhante

A Lei do Cibercrime veio introduzir novidades relativamente à temática da prova digital.

Nos termos do artigo 1.º, esta lei estabelece as disposições penais materiais e processuais relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico.

No capítulo III sobre "disposições processuais", a lei veio estabelecer um conjunto de novos meios de obtenção de prova.

Porém, primeiramente, cabe definir o âmbito de aplicação destas disposições

O artigo 11.º estabelece que as regras processuais previstas, com exceção do disposto no artigo 18.º, referente à interceção de comunicações, e no artigo 19.º, referente às ações encobertas, se aplicam: a) A processos relativos aos crimes previstos na própria lei, nos artigos 3.º a 8.º; b) A processos relativos a crimes cometidos por meio de um sistema informático como, por exemplo, a burla informática, prevista no artigo 221.º do Código Penal; c) A processos relativos a crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

A Lei do Cibercrime compreende, assim, um regime geral sobre recolha de prova em suporte eletrónico, aplicável a processo por qualquer crime, desde que, de alguma forma, este crime se relacione com o meio informático.

[69] NUNES (a) (2018), p. 25

[70] RODRIGUES (2008), p. 60

Relativamente ao caso concreto de apreensão de correio eletrónico e registos de comunicações de natureza semelhante, o instrumento legal estabelece um regime especial no artigo 17.º, ao dispor que "quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal".

Cabe referir que esta norma se aplica a mensagens de correio eletrónico ou a registos de comunicações de natureza semelhante, recolhidos no decurso de uma pesquisa informática, ou de outro acesso legítimo a um sistema informático.

Para Paulo Dá Mesquita[71], o conceito de "correio eletrónico" "é amplo, abrangendo tanto os sistemas que utilizam o conglomerado de redes eletrónicas de escala mundial (…) como sistemas de redes de computadores privados."

Relativamente ao acesso legítimo, neste contexto inclui a realização de perícias, quando estas sejam realizadas antes da apreensão, bem como o acesso a dados que estejam na disponibilidade ou controlo de outra entidade (nos termos do número 1 do artigo 14.º).[72]

Porém, a maior incerteza relativamente a este preceito prende-se com o facto de o artigo 17.º da Lei do Cibercrime remeter expressamente para a aplicação do regime das apreensões, regulado nos artigos 179.º a 252.º do Código de Processo Penal.

Acresce que, nos termos do artigo 189.º do CPP, "o disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes."

Logo, aparentemente, o Código de Processo Penal estabelece no artigo 189.º que estas comunicações devem seguir as regras processuais aplicáveis às escutas telefónicas.

Assim, levanta-se a questão de determinar como se devem conjugar estes regimes distintos, perante a multiplicidade de respostas possíveis.

7.1 Necessidade de articulação da Lei do Cibercrime com as normas do Código de Processo Penal: algumas questões problemáticas

Efetivamente, perante esta estipulação pouco esclarecedora, o regime previsto no artigo 17.º da Lei do Cibercrime tem gerado dificuldades de compatibilização com o disposto no Código de Processo Penal e tem resultado em interpretações doutrinais e jurisprudenciais diversas.[73]

Destaca-se, desde logo, a necessidade de determinar como se deve articular a previsão do artigo 189.º do CPP com o artigo 17.º da Lei da Cibercrime, na medida em que, enquanto o primeiro

[71] MESQUITA (2010), p. 121
[72] CARDOSO (2018), p. 179
[73] FIDALGO (2019) (a), p. 68

preceito estabelece que se deve sujeitar as comunicações por correio eletrónico ou outras formas de transmissão de dados por via telemática à aplicação das normas inerentes às escutas telefónicas, já a previsão da Lei do Cibercrime remete a apreensão das comunicações por correio eletrónico e registo de comunicações para o regime das apreensões em geral.

Cabe destacar o Acórdão do Tribunal da Relação de Évora de 20.01.2015[74], processo 648/14.6GCFAR-A.E1, que estabelece que "o regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão às «telecomunicações eletrónicas», «crimes informáticos» e «recolha de prova eletrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. (…) Para a prova eletrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime (…) Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual «geral» do cibercrime e da prova eletrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009. 5. As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder á recolha de prova em suporte electrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem à pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere á intercepção de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo às disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova electrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita)."

Seguindo esta orientação, é pacífico considerar que o regime da Lei do Cibercrime se categoriza enquanto regime geral nesta matéria específica, visto que esta temática, ao não se encontrar especificamente regulada no Código de Processo Penal, se sobrepõe às normas processuais penais.

Consequentemente, é de defender a aplicação do artigo 17.º enquanto norma primordial no contexto da apreensão das comunicações por correio eletrónico ou registo de comunicações semelhantes, devendo aplicar-se, subsidiariamente, tal como o próprio preceito da Lei do Cibercrime prevê, o artigo 179.º Código Processo Penal, ou seja, o regime da apreensão de correspondência.

Simultaneamente, é ainda passível de considerar que o n.º 1 do artigo 189.º do Código de Processo Penal, ainda que se mantenha inalterado, foi tacitamente revogado pelos artigos 17.º e 18.º da Lei

[74] Acórdão do Tribunal da Relação de Évora de 20.01.2015 (João Gomes de Sousa), in http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument.

do Cibercrime na parte em que se refere a correio eletrónico e registos de comunicações semelhantes, na medida em que já não é aplicável a equiparação da apreensão de correio eletrónico às escutas telefónicas.[75]

O regime suscita ainda a necessidade de determinar a que crimes se aplicam as respetivas estipulações.

Nos termos da alínea b) do artigo 179.º, n.º 1, do Código de Processo Penal, relativo à apreensão de correspondência, o juiz só pode autorizar ou ordenar a apreensão de correspondência, sendo o juiz que autoriza ou ordena a diligência, quando estiver em causa um crime punível com pena de prisão superior, no seu máximo, a 3 anos.

Nos termos do número 3 da mesma norma, o juiz que tiver autorizado ou ordenado a apreensão é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida

Se o juiz considerar que a correspondência apreendida é relevante para a prova, determina que esta seja junta ao processo.[76]

Caso contrário, restitui-a ao seu titular, não podendo ser utilizada enquanto meio de prova. Todavia, quanto ao pressuposto relativo ao crime em causa — crime punível com pena de prisão superior, no seu máximo, a 3 anos –, o problema que se coloca impõe-se, desde logo, pelo facto de alguns dos tipos legais de crimes previstos na Lei do Cibercrime não serem puníveis com penas de prisãosuperiores a 3 anos.

Tal como já foi previamente referido, o artigo 11.º da Lei do Cibercrime, ao delimitar o âmbito de aplicação das disposições processuais, estabelece que, com exceção do disposto relativamente a interceção de comunicações e a ações encobertas, as ditas disposições previstas na Lei do Cibercrime se aplicam a processos relativos aos crimes previstos na própria lei, a processos relativos a crimes cometidos por meio de um sistema informático e ainda a processos relativos a crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

Através da exceção que se prevê relativamente à interceção de comunicações e à admissibilidade de recurso a ações encobertas, o legislador refere expressamente que tais meios processuais podem ser utilizados em processos relativos a crimes previstos na Lei do Cibercrime e noutros processos por crimes que integrem o catálogo de crimes referido em cada uma das normas.[77]

Logo, aparenta ter sido opção ponderada por parte do legislador permitir expressamente que a apreensão de correio eletrónico e registos de comunicações de natureza semelhante possam ocorrer no âmbito de diversos tipos legais, sem a limitação decorrente de o crime ser punível com pena de prisão superior a 3 anos.[78]

Perante o silêncio da lei, ao não estabelecer nenhuma estipulação especial, aparenta permitir-se a utilização deste meio de obtenção de prova em processos relativos aos crimes previstos na própria Lei do Cibercrime, conforme resulta do âmbito de aplicação geral do instrumento legal.[79]

Questão distinta passa por determinar se a intenção do legislador seria a de que a apreensão de correio eletrónico fosse utilizada em qualquer processo, por qualquer crime, em relação ao qual

[75] NUNES (a) (2018), p. 26
[76] FIDALGO (2019) (a), p. 156 e ss
[77] FIDALGO (2019) (a), p. 156 e ss.
[78] NEVES (2011), p. 274 – 276
[79] NEVES (2011), p. 275

seja necessário proceder à recolha de prova em suporte eletrónico.

Porém, ao estabelecer na alínea c) do artigo 11 que as disposições processuais se aplicam a processos relativos a crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, o legislador aparenta ter conferido uma grande margem de liberdade à entidade investigadora, possibilitando à aplicação destas normas processuais aos crimes em relação aos quais seja "necessário proceder à recolha de prova em suporte eletrónico".

Ao estipular um regime tão abrangente, sem clarificar em que consiste o conceito de necessidade neste contexto específico, o legislador acaba por conferir um grande grau de discricionariedade à entidade que regula a investigação, facilitando a aplicação da Lei do Cibercrime a um número vasto de tipos legais e situações fácticas.

Outra questão que se tem colocado está relacionada com a exigência de despacho judicial prévio, que autorize ou ordene a apreensão de mensagens de correio eletrónico[80].

As respostas doutrinais têm sido diversas.

Enquanto Rita Castanheiro Neves[81] considera que a apreensão só pode ser feita na sequência de um despacho judicial, Pedro Verdelho[82] clarifica que a lei não é expressa a este propósito e que permite que se proceda a uma apreensão cautelar ou provisória de mensagens de correio eletrónico, ainda que não se tenha verificado a elaboração de um despacho judicial anterior.

Esta apreensão será provisória porque as mensagens só serão efetivamente apreendidas e juntas ao processo se o juiz assim determinar.

Se o juiz não autorizar a apreensão, então "a apreensão não se mantém, devendo o suporte de as mensagens em causa ser devolvido ou, se a apreensão tiver sido feita por cópia, destruído".[83]

Se considerarmos a aplicabilidade prática desta apreensão, a opinião de Pedro Verdelho aparentemente vai mais ao encontro de exigências e necessidades práticas.

Efetivamente, por regra, estas mensagens são apreendidas no decurso de pesquisas informáticas, que têm lugar no âmbito de buscas.

O autor salienta que, tendencialmente, antes de uma busca ainda não se sabe qual vai ser o resultado da referida busca, muito menos se vai conduzir a alguma apreensão: os órgãos de polícia criminal não sabem se vão encontrar um computador ou um dispositivo semelhante, se do referido dispostito consta mensagens e se as mensagens em causa são relevantes para o decurso da investigação.

Assim, segundo o autor, devemos considerar que a lei permite que se faça uma apreensão provisória de mensagens de correio eletrónico ou comunicações semelhantes, no âmbito de pesquisas informáticas realizadas, por exemplo, com autorização do Ministério Público, sendo depois tais mensagens presentes ao juiz, para que este ordene a respetiva apreensão e junção ao processo.

Porém, apesar de ser impossível discordar desta perspetiva de um ponto de vista estritamente de aplicabilidade prática, pois efetivamente acabaria por facilitar e beneficiar bastante as investigações, a verdade é que não é possível ignorar as previsões legais, sendo que a lei apresenta

[80] FIDALGO (2019) (b), p. 157
[81] NEVES (2011), p. 274 – 276
[82] VERDELHO (2009), p. 743
[83] VERDELHO (2009), p. 743

expressamente a sua solução para esta questão.

Para além da remissão expressa para o regime da apreensão de correspondência, previsto no artigo 179.º do CPP, o próprio artigo 17.º da Lei do Cibercrime estabelece que, quando forem encontradas mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a sua apreensão.

Acresce que, perante a eventual restrição do direito da inviolabilidade da correspondência, a única maneira de salvaguardar a necessidade dessa restrição é através despacho judicial prévio.

Neste sentido, segue também a jurisprudência nacional.

De ressalvar o Acórdão do Tribunal da Relação de Lisboa de 11.01.2011[84] processo n.º 5412/08.9TDLSB-A.L1-5, que estabelece que "As mensagens de correio electrónico ou registos de comunicações de natureza semelhante, que se afigurem de grande interesse para a descoberta da verdade ou para a prova, podem ser apreendidas, aplicando-se correspondentemente o regime de apreensão de correspondência previsto no CPP; Tais apreensões têm de ser autorizadas ou determinadas por despacho judicial, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, sob pena de nulidade".

De acordo com este entendimento, o Acórdão do Tribunal da Relação de Lisboa de 06.02.2018[85], processo n.º 1950/17.0T9LSB-A.L1-5, considera que "Aplicando-se assim o regime de apreensão de correspondência previsto no Código de Processo Penal, este encontra-se disciplinado no art.º 179º, o qual estabelece desde logo no n.º 1 que tais apreensões sejam determinadas por despacho judicial, "sob pena de nulidade" expressa (n.º 1)".

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

Esta questão remete para uma verdadeira discussão de qual é o papel do Juiz de Instrução Criminal e as competências que lhe são atribuídas, comparativamente ao papel do Ministério Público.

O número 3 do artigo 179.º do Código de Processo Penal refere que o juiz que autorizou a apreensão de correspondência deve ser o primeiro a ter conhecimento do conteúdo específico da apreensão. Como já foi referido ao longo desta dissertação, é o próprio artigo 17.º da Lei do Cibercrime que remete para a aplicabilidade das regras específicas do Código de Processo Penal.

Na esfera defendida por Pedro Verdelho[86], através de uma interpretação não restritiva, a lei não exige que o juiz seja o primeiro a tomar conhecimento do conteúdo das mensagens apreendidas, permitindo que a entidade que procede à pesquisa encaminhe posteriormente para o juiz mensagens concretas que aquele depois apreenderá ou não, consoante o interesse para o processo.

Segundo esta doutrina, também defendida por Rui Cardoso, considerar que o juiz de instrução deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico ou semelhantes apreendidas põe em causa a própria coerência do sistema de tutela de direitos.

De facto, cabe refletir sobre a circunstância de, nos casos de interceção de comunicações (artigo

---

[84] Acórdão do Tribunal da Relação de Lisboa de 11.01.2011 (Ricardo Cardoso), in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument.

[85] Acórdão do Tribunal da Relação de Lisboa de 06.02.2018 (João Carrola), in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument.

[86] VERDELHO (2009), p. 744.

18.º da Lei do Cibercrime), potencialmente mais lesiva de direitos fundamentais, se permitir que os órgãos de polícia criminal e o Ministério Público sejam os primeiros a tomar conhecimento do conteúdo das comunicações.[87]

Já Rita Castanheira Neves[88], numa tentativa de defender uma posição mais moderada, reconhece a dificuldade do cumprimento da exigência legal prevista no número 3 do artigo 179.º, alegando principalmente a quantidade por vezes excessiva de e-mails apreendidos.

Neste sentido, a autora defende a eventual possibilidade de apreensão dos e-mails que se revelem determinantes para a produção de prova por parte dos órgãos de polícia criminal.

A autora admite a existência de uma pré-seleção por parte dos órgãos de polícia criminal, recorrendo a técnicas de pesquisa, nomeadamente através da uma procura circunscrita a determinados elementos como palavras-chaves, período de datas ou um remetente concreto.

Contudo, a jurisprudência não tem necessariamente acolhido este entendimento.

Cabe destacar a posição jurisprudencial maioritária que defende que estão em causa direitos constitucionalmente previstos, designadamente o direito à privacidade e ao sigilo da correspondência eletrónica, considerando aplicável o regime de apreensão de correspondência do Código de Processo Penal, que estabelece que "o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida".

De facto, alguns tribunais têm entendido que, efetivamente, o juiz que autoriza ou ordena a diligência deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio eletrónico apreendidas.

Neste sentido, cabe destacar o Acórdão do Tribunal da Relação de Lisboa de 27.01.2021[89], processo 184/12.5TELSB-R.L1-3, que considera que "é de aplicar o disposto no artigo 17.º da Lei do Cibercrime, tudo se processando como se de uma apreensão de correspondência nos termos do CPP se tratasse; Sendo, ab initio, autorização judicial para tal; Se assim for, a correspondência apreendida terá de ser presente e seleccionada por um juiz antes de ser junta ao processo e poder aí ser considerada; A omissão desta formalidade constitui nulidade e acarreta a inadmissibilidade da prova obtida".

No mesmo sentido, o Tribunal Constitucional[90] considera que o juiz deve ser o primeiro a ter conhecimento do conteúdo, salvo se existir uma justificação cabal, robusta e bem determinada que justifique a aplicação de uma solução distinta, não podendo exceder os limites inerentes a qualquer solução excecional.

Por fim, cabe referir a problemática inerente a uma possível distinção de regime conforme se trate de apreensão de conteúdo aberto e lido, conteúdo ainda não lido ou conteúdo em trânsito.

A este propósito, é imperativo proceder a uma análise do Acórdão do Supremo Tribunal de Justiça nº 10/2023.

---

[87] CARDOSO (2018), p. 197 e ss

[88] NEVES (2011), p. 275

[89] Acórdão do Tribunal da Relação de Lisboa de 27.01.2021 (Rui Miguel Teixeira), in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1beb942c43eaa700802586760032418f?OpenDocument.

[90] Acórdão do Tribunal Constitucional n.º 687/2021 de 22.09.2021, in https://diariodarepublica.pt/dr/detalhe/acordao-tribunal-constitucional/687-2021-171674458

8. Análise do Acórdão do Supremo Tribunal de Justiça n.º 10/2023 de 10.11.2023

8.1. Identificação da questão jurídica

O Supremo Tribunal de Justiça, no Acórdão de Fixação de Jurisprudência de 10.11.2023[91], determinou que apenas o juiz de instrução tem competência para apreender mensagens de correio eletrónico.

A apreensão de correio eletrónico e registos de comunicação de natureza semelhante, regulada nos termos do artigo 17.º da Lei do Cibercrime, foi sempre controversa, nomeadamente quanto à eventual necessidade de proceder a uma distinção entre correio eletrónico aberto e fechado.

Ainda que, em primeira análise, esta questão aparente remeter para um mero preciosismo linguístico-jurídico, no contexto prático impacta significativamente inúmeros processos de investigação.

A questão que se coloca remete para uma eventual distinção entre e-mails já abertos ou lidos e e-mails fechados ou não lidos, o que, consequentemente, acabaria por se traduzir na aplicação de regimes distintos consoante as circunstâncias do caso concreto, mais concretamente a aplicação ou afastamento do artigo 17.º da Lei do Cibercrime.

Neste sentido, o Acórdão do Tribunal da Relação de Lisboa de 27.01.2021[92], processo 184/12.5TELSB-R.L1-3, considerou que, tal como a correspondência em papel, a correspondência digital segue regimes de apreensão diferentes consoante a mesma ainda não haja sido remetida, tenha sido remetida e esteja em trânsito, haja sido recebido e não lida ou haja sido recebida e lida.

De acordo com esta posição jurisprudencial, nas situações em que a correspondência haja sido recebida, mas ainda não haja sido lida pelo destinatário é de aplicar o disposto no artigo 17.º da Lei do Cibercrime, tudo se processando como se de uma apreensão de correspondência nos termos do Código de Processo Penal se tratasse.

Por outro lado, nas situações em que a mensagem está em trânsito e for intercetada é de aplicar o artigo 18.º da Lei do Cibercrime, referente à interceção de comunicações.

Já nas situações em que a correspondência já tenha sido recebida e lida é de aplicar o disposto no artigo 16.º da Lei do Cibercrime, referente à apreensão de dados informáticos.

Nestas situações, a apreensão pode ser ordenada pelo Ministério Público e por este executada não sendo necessária qualquer autorização judicial prévia à busca ou validação judicial subsequente da mesma.

Esta posição jurisprudencial encontra apoio entre a doutrina nacional.

De acordo com a opinião perfilhada por João Correia[93], Paulo Mesquita[94] e Duarte Nunes[95], o

---

[91] Acórdão do Supremo Tribunal de Justiça de 10.11.2023 (Pedro Branquinho Dias), in https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/10-2023-224081976

[92] Acórdão do Tribunal da Relação de Lisboa de 27.01.2021 (Rui Miguel Teixeira), in https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1beb942c43eaa700802586760032418f?OpenDocument

[93] CORREIA (2014), p. 41

[94] MESQUITA (2010), p. 118

[95] NUNES (b) (2018), p. 145-146

correio eletrónico recebido e lido deverá ser excluído do regime do artigo 17.º da Lei do Cibercrime[96].

Sendo passível de ser considerado um mero documento, a sua apreensão deverá ser feita nos termos do regime da apreensão de dados informáticos, sendo suficiente a intervenção do Ministério Público com possibilidade de controlo judicial posterior, sempre que o conteúdo dos documentos apreendidos for suscetível de revelar dados pessoais ou íntimos que possam pôr em causa a privacidade do respetivo titular ou de terceiro, seguindo o regime previsto nos números 1 e 3 do artigo 16.º da Lei do Cibercrime[97].

No entendimento de Manuel da Costa Andrade[98], "depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito", sujeitando-se ao mesmo regime a que ficam sujeitos os documentos arquivados em qualquer dispositivo eletrónico.

Acresce que, segundo estes autores, o regime especial previsto no artigo 17.º da Lei do Cibercrime apenas se justifica em relação a mensagens de correio eletrónico ainda não lidas pelo seu destinatário.

Por seu turno, Rita Castanheira Neves[99] segue uma posição diversa, ao defender que a ingerência nas mensagens de correio eletrónico ou registos de natureza semelhante deverá ser objeto de um duplo tratamento: enquanto interceção nas comunicações, em tempo real e, enquanto comunicações armazenadas em suporte digital.

Todavia, cabe questionar, perante a leitura da norma, se o legislador, ao referir-se apenas a "mensagens de correio eletrónico ou registos de comunicações de natureza semelhante", sem qualquer indicação de decurso temporal ou de interação com as mensagens por parte do recetor, não demonstrou claramente a sua intenção de submeter toda a apreensão de correio eletrónico e registos de comunicações de natureza semelhante ao regime da apreensão da correspondência[100], independentemente das mensagens se encontrarem lidas ou não lidas.

Como refere Rui Cardoso, a analogia entre correspondência aberta ou não aberta, facilmente verificável na correspondência tradicional por corresponder a um bem corpóreo, não é passível de ser aplicável no plano digital.[101]

Efetivamente, no caso do correio eletrónico ou de mensagens enviadas através de qualquer serviço, não aparenta existir qualquer diferença em estar aberto ou fechado, lido ou não lido[102].

Através do desenvolvimento da tecnologia, um e-mail ou uma mensagem equiparada podem ser abertos num dispositivo e, após se proceder à sua leitura, proceder à marcação dos mesmos como não lidos.

Estando perante a possibilidade de existência de vários dispositivos pertencentes ao mesmo indivíduo, pode ainda acontecer que uma mensagem apresentada como não lida, tenha eventualmente sido aberta e lida noutro dispositivo.

---

[96] FIDALGO (2019) (b), p. 159
[97] FIDALGO (2019) (b), p. 159
[98] ANDRADE (2009) (b), p. 157
[99] NEVES (2011), p. 278
[100] RAMALHO (2017), p. 278
[101] CARDOSO (2018), p. 179
[102] BRANCO (2021), p. 36

Assim, ao remeter-se ao silêncio, não especificando se o artigo 17.º se aplica apenas a mensagens lidas ou não lidas, o legislador aparenta ter procurado não traçar uma fronteira que, perante a tecnologia, não é fácil de estabelecer.

Neste sentido, o Acórdão do Tribunal da Relação de Lisboa de 07.03.2018[103], processo 184/12.5TELSB-B.L1-3, determina que "a redacção do artº 17º da LC resulta de forma clara que não esteve no espírito do legislador transpor para o correio electrónico e registos de comunicações de natureza semelhante a distinção, por referência ao correio tradicional, de correio aberto ou fechado, o que desde logo se colhe do elemento literal previsto neste preceito legal com a expressão "armazenados" o que pressupõe que a comunicação já foi recebida/lida e, consequentemente, armazenada, além de não existirem razões para considerar diminuídas as exigências garantísticas do correio electrónico quando aberto/lido relativamente ao correio electrónico fechado, atenta a natureza própria destas comunicações.".

No mesmo sentido, o Acórdão do Tribunal da Relação de Lisboa de 15.06.2022, processo n.º 10626/18.0T9LSB-B.L1-PICRS, ao estabelecer que "A propósito desta problemática, vem questionado se existe distinção juridicamente relevante entre correspondência digital aberta e fechada e se apenas esta será merecedora de particular tutela legal e constitucional, cabendo aquela na mole genérica de «documentos» (…). A este respeito, importa começar por referir que a questão não tem o menor suporte na letra do mencionado artigo 17.º da LC o que logo convoca o brocardo latino «ubi lex non distinguit nec nos distinguere debemus». Com efeito, o legislador não fez tal distinção entre correspondência lida ou por ler. Do texto do referido artigo antes se extrai que o criador da norma quis proteger a correspondência digital em qualquer estado do processo comunicacional e até após o termo deste, fazendo englobante menção a «mensagens de correio eletrónico ou registos de comunicações de natureza semelhante». À luz desse diploma legal, não tem suporte qualquer tentativa de separação conceptual e classificativa."

De facto, a jurisprudência e a doutrina portuguesa, têm revelado dificuldades em adotar uma posição uniforme relativamente a esta questão interpretativa.

Consequentemente, verificou-se a aplicação de soluções distintas com base em duas posições maioritárias contraditórias.

A primeira posição remete para a ideia de que, quando uma mensagem de correio eletrónico já se encontra aberta, presumindo-se que foi lida e se encontra na esfera de conhecimento do destinatário, encontrando-se armazenada no sistema informático, perde a natureza de correspondência e assume a condição de mero documento digital.

Consequentemente, a sua apreensão remete para o regime previsto no artigo 16.º da Lei do Cibercrime e não carece de autorização judicial.

Por outro lado, a posição jurisprudencial contrária defende a aplicabilidade do artigo 17.º da Lei do Cibercrime a toda e qualquer mensagem de correio eletrónico, considerando que só o juiz de instrução pode apreender a correspondência eletrónica.

Assim, perante a impossibilidade de responder de forma clara às questões suscitadas, surgiu a necessidade de pronunciamento por parte do Supremo Tribunal de Justiça, com a finalidade de

[103] Acórdão do Tribunal da Relação de Lisboa de 07.03.2018 (Conceição Gonçalves), in https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument

esclarecer as dúvidas interpretativas existentes.

8.2. Breve exposição da factualidade do caso concreto

Com relevância para a presente dissertação, as circunstâncias o caso concreto são as seguintes[104]:

a) Por despacho proferido a 24.05.2017 foram emitidos mandados de busca não domiciliária por parte do MP às instalações da E…, tendo como alvos, entre outros, o arguido e recorrente.

b) No despacho em causa fez-se constar expressamente que as buscas deveriam incidir sobre toda a documentação encontrada nos respetivos postos de trabalho e arquivos utilizados pelos visados, incluindo toda a que se encontra em formato digital, ainda que se trate de documentos originados ou recebidos via correio eletrónico.

c) Na sequência de tal despacho, a PJ cumpriu o mandato a 02.06.2017, tendo realizado as referidas buscas.

d) Por despacho proferido a 09.06.2017, os dados apreendidos em suporte digital na realização das buscas foram remetidos ao JIC, para exame e decisão sobre a sua junção aos autos nos termos do artigo 17º da LC, artigo 179.º, n.º 3 e 188.º, nºs 1 e 4 do CPP, junção essa que acabou por ocorrer.

e) Após vicissitudes várias, o arguido vem requerer a nulidade dos despachos do MP, entre outros, do despacho proferido a 14.08.2020, pelo qual foi ordenada a junção aos autos, para serem utilizadas e valoradas enquanto meio de prova as mensagens de correio eletrónico apreendidas

f) Por despacho de 23.09.2020, o Tribunal decide indeferir a invocada proibição de prova resultante da seleção de mensagens de correio.

f) O arguido, nos termos das disposições conjugadas dos artigos 437.º, n.ºs 2, 3, 4 e 5 e 438.º, n.ºs 1 e 2 do CPP, interpôs recurso extraordinário para a fixação de jurisprudência do Acórdão do Tribunal da Relação de Lisboa de 27.01.2021, que julgou improcedente o seu recurso do despacho proferido em 23.09.2020 pelo Juiz de Instrução do Tribunal Central de Instrução Criminal.

g) O Acórdão recorrido encontra-se em manifesta oposição sobre a mesma questão jurídica com o Acórdão do Tribunal da Relação de Lisboa de 07.03.2018.

h) A questão jurídica em causa consistia em determinar se a circunstância de uma mensagem de correio eletrónico se mostrar sinalizada como aberta ou lida, no momento da respetiva apreensão, afastava a aplicação do artigo 17.º da LC, ou se, por outro lado, essa circunstância é irrelevante, aplicando-se o regime do artigo 17.º da LC a todas e quaisquer mensagens de correio eletrónico apreendidas.

---

[104] Acórdão do Supremo Tribunal de Justiça de 10.11.2023 (Pedro Branquinho Dias), in https://diariodarepublica.pt/dr/detalhe/acordao-supremo-tribunal-justica/10-2023-224081976

i) O Acórdão recorrido entendeu que o regime aplicável ao caso seria o previsto no artigo 16.º da LC, o que atribui ao MP a competência para seriar as mensagens empreendidas e determinar qual o material probatório relevante para a investigação, na medida em que, encontrando-se os e-mails em causa abertos, apenas correspondem a meros documentos digitais.

j) O Acórdão fundamento entendeu que as mensagens do correio eletrónico se encontrem armazenadas num sistema informático, independentemente de encontrar abertas ou fechadas, devem seguir o regime previsto no artigo 17.º da LC, ou seja, só podem ser apreendidas mediante despacho prévio do JIC, devendo o juiz ser a primeira pessoa a tomar conhecimento do conteúdo da correspondência.

8.3 Exposição da questão jurídica

O Tribunal inicia a sua análise mediante uma clarificação dos poderes do Ministério Público do juiz de instrução em fase de inquérito.

De facto, a direção do inquérito cabe ao Ministério Público que, em consequência da estrutura acusatória ao processo penal, prevista no número 5 do artigo 32.º da Constituição da República Portuguesa, e da autonomia constitucional atribuída ao Ministério Público, nos termos do número 2 do artigo 219.º da Constituição da República Portuguesa, exerce a função de *dominus processus*.

Por sua vez, nos termos do artigo 268.º do Código de Processo Penal, consagram-se determinados atos cuja prática, na fase de inquérito, é da competência do juiz de instrução, sendo que a maioria destas competências provém da posição do juiz de instrução enquanto juiz garante de liberdades, garantias e direitos.

De referir que nos termos do número 2 do referido preceito o juiz pratica os atos referidos a requerimento do Ministério Público, da autoridade de polícia criminal em caso de urgência ou de perigo na demora, do arguido ou do assistente.

De facto, a intervenção do juiz de instrução na fase de inquérito é ocasional provocada e tipificada, em consonância com a estrutura acusatória do processo penal português, na medida em que a entidade que investiga é distinta da entidade que julga.

Assim, de acordo com a análise do Tribunal, a prática pelo juiz de instrução de atos que atingem direitos, liberdades e garantias, na fase de inquérito, depende do impulso do Ministério Público.

Por outro lado, no artigo 269.º do Código de Processo Penal enumeram se as diligências que cabe exclusivamente ao juiz de instrução ordenar ou autorizar.

Perante a relevância para o caso em apreço, cabe destacar alínea d) do número 1 do referido preceito, que estabelece que, durante o inquérito, compete exclusivamente ao juiz de instrução ordenar ou autorizar apreensões de correspondência, nos termos do número 1 do artigo 179.º.

Como este preceito remete para atos efetivamente limitativos de direitos fundamentais é da competência exclusiva do juiz de instrução, enquanto juiz das liberdades, garantias e direitos, ordenar ou autorizar estes atos.

Todavia, o Tribunal recorda que, considerando a posição processual do juiz, não pode tomar a iniciativa para a prática destes atos.

Ultrapassada esta questão introdutória relativa aos poderes do Ministério Público e do Juiz de Instrução Criminal, o Tribunal inicia a análise concreta da apreensão de correio eletrónico ou de outros registos de comunicações de natureza semelhante.

Cabe ressalvar que o regime legal da apreensão de correspondência e, particularmente, do correio eletrónico, encontra-se em conflito com o direito fundamental à inviolabilidade do domicílio da correspondência que, nos termos do número 4 do artigo 34.º da Constituição, estabelece a proibição de "ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal".

O Tribunal considera que este preceito "visa proteger a liberdade de manter uma esfera de privacidade e sigilo livre de interferência ingerência estadual".

Avançando para a análise do artigo 17.º da Lei do Cibercrime, o Tribunal rapidamente conclui que "na letra e no espírito deste preceito, a apreensão de correio eletrónico e de outros registos de comunicações de natureza semelhante terá de ser sempre autorizado ordenada pelo juiz de instrução, pelo que, sendo encontradas num sistema informático ou em suporte autónomo legitimamente acedidos, mensagens de correio eletrónico ou realidades análogas cuja aquisição tenha grande interesse para a investigação e descoberta da verdade, terá de ser requerida ao juiz a autorização para a sua apreensão.".

O Tribunal legitima a sua posição na necessidade de salvaguardar os direitos fundamentais que são diretamente afetados por esta faculdade processual, designadamente o direito à intimidade da reserva da vida privada e à privacidade, o direito à palavra e o direito à autodeterminação informacional.

Acresce ainda a necessidade de uma eventual restrição destes direitos depender da verificação dos requisitos da adequação necessidade e proporcionalidade, na vertente de proibição do excesso, o que só poderá ser garantido por parte do juiz de instrução criminal, enquanto juiz garante de direitos liberdades e garantias.

No entanto, o Tribunal esclarece que, ainda que o artigo 17.º da Lei do Cibercrime consagre uma remissão para o regime da correspondência corpórea, a sua aplicação nunca poderá ser integral, só devendo ser concretizada no âmbito de conteúdo que não contraria a Lei do Cibercrime, ou seja, a remissão para as normas do Código de Processo Penal não se sobrepõe ao regime especial.

Neste sentido, o Tribunal defende a não aplicação do número 3 do artigo 179.º do Código de Processo Penal o que, aparentemente, se traduz na desnecessidade de o juiz de instrução ser o primeiro a tomar conhecimento do conteúdo da correspondência.

Efetivamente, o correio eletrónico apresenta características muito distintas do correio tradicional, o que justifica a discrepância em termos de regimes.

Por consequente, não faz verdadeiramente sentido distinguir entre as mensagens abertas e fechadas no âmbito do correio eletrónico ou registos de comunicações de natureza semelhante, visto que, ao contrário do que sucede no âmbito do correio tradicional é praticamente impossível determinar, de forma séria e verdadeira, se uma mensagem já foi ou não lida.

Acresce que a garantia constitucional de inviolabilidade das comunicações abrange as mensagens de correio eletrónico enquanto permanecerem no sistema informático, independentemente de a mensagem ter sido ou não aberta.

Nas palavras do Tribunal, "a distinção entre mensagens abertas e fechadas é, neste âmbito, em bom rigor, artificial e falível".

Conclui-se que a intervenção do juiz de instrução, enquanto juiz garante dos direitos, liberdades e garantias é considerada sempre imprescindível no âmbito da apreensão de mensagens armazenadas em sistema informático, independentemente de as mensagens se encontrarem ou não assinaladas como abertas.

Contudo, o Tribunal alerta para o facto de as divergências relativas à interpretação do artigo 17.º

remeterem para uma eventual obrigatoriedade de existência de um despacho prévio do juiz de instrução, que autorizasse ordenasse a apreensão das mensagens, assim como a tomada de conhecimento do conteúdo das mensagens pelo juiz em primeiro lugar.

Perante uma análise em sentido estrito, na medida em que o preceito não menciona uma eventual possibilidade de apreensão cautelar ou provisória das mensagens de correio eletrónico, é facilmente defensável a necessidade de ser o juiz a primeira entidade a tomar conhecimento das mensagens cabendo-lhe, naturalmente, ordenar a junção ou não das mesmas ao processo.

Porém, o Tribunal adota uma perspetiva que considera as necessidades do sistema, designadamente as situações de perigo da demora, sendo passível considerar que as autoridades, o Ministério Público e os órgãos de polícia criminal, possam recorrer à medida cautelar estabelecida no artigo 252.º do Código de Processo Penal.

Nessa circunstância, a ordem dada ao fornecedor de serviço de não remessa do correio eletrónico para o destinatário carecerá de validação posterior através de despacho fundamentado do juiz de instrução no prazo de 48 horas.

O tribunal termina a sua análise com a ressalva de que, não sendo a lei totalmente clara, perante a diversidade de regimes, entendo que a solução mais adequada remete para a aplicação do artigo 17.º da Lei do Cibercrime a toda e qualquer mensagem de correio eletrónico, justificante a mesma proteção constitucional independentemente do conteúdo da Mensagem se encontrar lido ou não lido.

Os Juízes Conselheiros que constituem as Secções do Supremo Tribunal de Justiça concluíram no sentido de julgar procedente o recurso extraordinário para fixação de jurisprudência interposto pelo arguido AA, revogando o acórdão recorrido, e fixar a seguinte jurisprudência: "Na fase de inquérito, compete ao juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente se encontrarem abertas (lidas) ou fechadas (não lidas), que se afigura em ser de grande interesse para a descoberta da verdade ou para a prova, nos termos do artigo 17.º, da Lei n.º 109/2009, de 15/09 (Lei do Cibercrime".

8.4. Análise e consequências da decisão

Primeiramente, cabe referir que um Acórdão Uniformizador de Jurisprudência corresponde a uma decisão proferida pelo Supremo Tribunal de Justiça que tem como objetivo primordial pôr termo a uma divergência ou contradição jurisprudencial.

Neste sentido, o Supremo Tribunal de Justiça procura determinar a solução para a problemática em que os tribunais de instância inferior divergiram, numa tentativa de adotar uma resposta constante que contribua para a segurança e certeza jurídica.

Ainda que os tribunais inferiores não fiquem formalmente vinculados a esta decisão, caso decidam em sentido contrário ao disposto no Acórdão de Uniformização de Jurisprudência, a parte vencida tem legitimidade e direito a interpor recurso com base neste fundamento.

Em consequência, verifica-se uma tendência entre os tribunais de instância inferior para decidir no sentido defendido pelo Supremo Tribunal de Justiça, de modo a irradiar as dúvidas existentes e contribuir para a estabilidade das decisões judiciais.

In casu, o Supremo Tribunal de Justiça considerou que a apreensão de correio eletrónico ou de registos de comunicações semelhantes é regulada por via do artigo 17.º da Lei do Cibercrime, independentemente de as mensagens se encontrarem fechadas e/ou não lidas ou abertas e/ou lidas.

Por conseguinte, a apreensão está dependente de um despacho judicial prévio.

Efetivamente, nos termos do número 2 do artigo 34.º da Constituição da República Portuguesa, o juiz de instrução criminal tem competência exclusiva, que não é delegável, para praticar todos e quaisquer atos de instrução que afetem diretamente os direitos fundamentais.

A lei constitucional impõe que, mediante uma restrição a direitos fundamentais, a intervenção do juiz de instrução, enquanto juiz garante dos direitos, liberdades e garantias, é considerada sempre imprescindível.

Qualquer restrição a direitos fundamentais deve ser a menor possível, limitando-se ao mínimo indispensável para assegurar apenas a efetiva prossecução dos bens e valores jurídicos em causa que justificam e legitimam a restrição desses direitos.

In casu, estamos perante a restrição de direitos fundamentais como a inviolabilidade da correspondência e de outros meios de correspondência privada, previsto no artigo 34.º da Constituição da República Portuguesa, a proteção de dados pessoais informáticos, previsto no artigo 35.º da Constituição da República Portuguesa, e a privacidade e reserva da intimidade da vida privada, previsto no artigo 26.º da Constituição da República Portuguesa, com o objetivo de prosseguir as finalidades da investigação criminal, designadamente a descoberta da verdade material, a realização da justiça e a restauração da paz jurídica.

Porém, a restrição destes direitos fundamentais deve limitar-se ao estritamente necessário para atingir essas finalidades.

O Ministério Público e o juiz de instrução têm, à luz da lei constitucional e da lei ordinária, natureza e funções fundamentalmente distintas.

O juiz de instrução criminal, enquanto figura independente, imparcial e garante máximo dos direitos, liberdades e garantias, representa uma garantia adicional de ponderação dos direitos e liberdades potencialmente atingidos no âmbito de uma investigação criminal.

Nas palavras do Tribunal Constitucional[105], "efetivamente, nos momentos processuais em que esteja em causa uma atuação restritiva das autoridades públicas no âmbito dos direitos fundamentais, a intervenção de um juiz - com as virtudes de independência e imparcialidade que tipicamente a caraterizam - é essencial para uma tutela efetiva desses direitos, mesmo nos casos em que estes devam parcialmente ceder, em nome da salvaguarda de outros bens constitucionalmente consagrados. O juiz tem, nos termos da Constituição, uma competência exclusiva e não delegável de garantia de direitos fundamentais no âmbito do processo criminal (à luz do artigo 32.º, n.º 4, do CPP), pelo que a lei apenas pode dispensar a sua intervenção em casos excecionais devidamente delimitados e justificados. Por outras palavras, tal dispensa é constitucionalmente admissível apenas em situações pontuais e definidas com rigor, em que não constitua um meio excessivo para prosseguir interesses particularmente relevantes de investigação criminal.".

Neste sentido, o Acórdão do Supremo Tribunal de Justiça pode determinar a nulidade de toda a prova que tenha sido adquirida mediante a apreensão de e-mails sem a autorização prévia do juiz de instrução, independentemente de os e-mails já terem sido lidos ou não.

Um despacho do Ministério Público que ordene a apreensão é nulo, nos termos do artigo 17.º da Lei do Cibercrime e 179.º, n.º 1, do Código de Processo Penal.

Acresce que esta determinação de nulidade é aplicável quer a casos futuros, quer a processos que ainda se encontram pendentes ou em tramitação.

---

[105] Acórdão do Tribunal Constitucional n.º 687/2021 de 22.09.2021, in https://diariodarepublica.pt/dr/detalhe/acordao-tribunal-constitucional/687-2021-171674458

De facto, com a pronúncia do Supremo Tribunal de Justiça no sentido de não existir qualquer diferença de tratamento entre e-mails abertos ou fechados, os arguidos cujos e-mails foram apreendidos sem autorização prévia do juiz de instrução, ou seja, mediante a exclusão do artigo 17.º da Lei do Cibercrime, ainda que os e-mails efetivamente já tivessem sido lidos no momento da apreensão, podem requerer a nulidade da prova, de forma a beneficiar da deliberação do Tribunal.

Assim, qualquer prova resultante de uma apreensão que não respeite os preceitos previamente mencionados constitui uma prova proibida, não podendo ser valorada nos termos dos artigos 18.º, n.º 8 e 34.º, nº 4 da Constituição da República Portuguesa, e 126.º, n.º 3 do Código de Processo Penal.

9. Conclusão

Concluída a exposição da investigação realizada, cumpre agora apresentar as respetivas conclusões.

A dissertação em apreço destinou-se a aprofundar a problemática da apreensão dos serviços de correio eletrónico e de comunicações semelhantes.

Procurou-se estabelecer linhas orientadoras que permitissem responder aos desafios inerentes a este meio de prova digital, com destaque para o Ac. do STJ n.º 10/2023, responsável por clarificar a problemática inerente a uma eventual distinção entre e-mails abertos ou lidos e e-mails fechados ou não lidos.

A dissertação iniciou-se com uma breve contextualização do sistema probatório português, através da distinção entre prova, meios de prova e meios de obtenção de prova. A prova é passível de ser definida como o esforço exigível para demonstrar fatos relevantes para a existência do crime e a aplicação de penas, enquanto os meios de prova correspondem ao caminho necessário para gerar convicção sobre esses fatos. Por sua vez, os meios de obtenção de prova correspondem aos instrumentos necessários para investigar e recolher os respetivos meios de prova.

Destaca-se ainda a relevância do princípio da legalidade da prova, que estabelece a admissibilidade de todas as provas que não sejam expressamente proibidas por lei.

Ultrapassada esta questão, revelou-se imperativo proceder a uma breve definição dos conceitos de cibercrime e prova digital. O cibercrime traduz-se num comportamento criminoso praticado em ambiente digital. Ademais, a prova digital remete para toda a informação, com valor probatório, armazenada ou transmitida, sob forma digital.

No que concerne especificamente aos serviços de correio eletrónico e de comunicações semelhantes, através da análise jurisprudencial apresentada foi possível ilustrar a variedade de situações em que estes meios de comunicação podem ser relevantes para a demonstração da existência de um crime. Cabe ressalvar a posição dos tribunais portugueses quanto à admissibilidade desses meios de prova, reconhecendo a sua importância como fontes probatórias, desde que obtidos legalmente e respeitando os direitos constitucionais vigentes.

Apesar da indiscutível relevância destes meios de prova no direito processual penal contemporâneo, coube refletir sobre a eventual colisão deste meio de prova com direitos fundamentais, designadamente o direito à reserva da intimidade da vida privada e familiar, o direito à inviolabilidade de meios de comunicação privada, da correspondência e das telecomunicações, e o direito à palavra. Destaca-se a necessidade de assegurar a existência de um regime que, de forma clara e inequívoca, respeite os direitos fundamentais dos cidadãos, mas que também permita

atingir os resultados necessários para a redução da criminalidade informático-digital.

A evolução legislativa inerente à apreensão de correio eletrónico e meios de comunicação semelhante procurou acompanhar as novas tecnologias e os novos desafios no processo penal.

Previamente à entrada em vigor da Lei do Cibercrime, não existiam disposições específicas inerentes a esta temática. A investigação dos crimes relacionados com a informática ocorria mediante a aplicação das previsões gerais do Código de Processo Penal.

Perante a ausência de regulamentação específica em matéria de apreensão de correio eletrónico, a doutrina e a jurisprudência maioritária defendiam a equiparação do correio eletrónico ao correio tradicional.

Por sua vez, na sistematização Código de Processo Penal de 1987, o legislador, no artigo 190.º, consagrou uma extensão da aplicação do regime das escutas "(…) às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone".

A Lei n.º 58/98 veio alterar este preceito, verificando-se, pela primeira vez, a regulação concreta deste meio de prova.

No entanto, foi apenas com a Lei do Cibercrime que se verificou a consagração de um regime específico que considerasse as suas características específicas.

Apesar do mérito atribuído a este instrumento jurídico, o artigo 17.º, que regula a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, suscita questões complexas, designadamente a articulação entre a Lei do Cibercrime e o Código de Processo Penal, a aplicação do regime de apreensão de correspondência, a necessidade de despacho judicial prévio e o papel do juiz na apreensão e valoração do conteúdo.

In casu, destaca-se a problemática da eventual necessidade de proceder a uma distinção entre correio eletrónico aberto e fechado, através da análise do Ac. STJ n.º 10/2023.

O caso em apreço remete a mandados de busca não domiciliária emitidos pelo Ministério Público, resultando na apreensão de documentos, incluindo mensagens de correio eletrónico. O arguido contesta a validade dessa apreensão, desencadeando um processo judicial.

O Tribunal conclui que a apreensão de mensagens de correio eletrónico deve sempre ser autorizada pelo juiz de instrução, independentemente de estarem abertas ou fechadas. Verifica-se uma tomada de posição que, ao estabelecer uma interpretação uniforme da lei, visa proteger os direitos fundamentais dos cidadãos

Esta decisão institui um precedente importante ao considerar que a apreensão de correio eletrónico ou de registos de comunicações semelhantes é regulada por via do artigo 17.º LC, independentemente de as mensagens se encontrarem fechadas e/ou não lidas ou abertas e/ou lidas.

Por conseguinte, a apreensão está dependente de um despacho judicial prévio.

Conclui-se que qualquer despacho do Ministério Público que ordene a apreensão é nulo, nos termos do artigo 17.º da LC e 179.º, n.º 1, do CPP.

Por fim, acresce que esta determinação de nulidade é aplicável quer a casos futuros, quer a processos que ainda se encontram pendentes ou em tramitação.

10. Bibliografia final

ANDRADE, Manuel da Costa, 2006, *Sobre as proibições de Prova em Processo Penal*, Coimbra Editora

ANDRADE, Manuel da Costa, 2009 (a), *A reforma do Código de Processo Penal*, Coimbra Editora

ANDRADE, Manuel da Costa, 2009 (b), *«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

BRANCO, José Ricardo Marques, 2021, *Prova Digital – Os meios de obtenção de Prova Digital e a restrição de direitos do arguido* [Dissertação de Mestrado, Faculdade de Direito da Universidade de Coimbra]. Disponível em https://estudogeral.sib.uc.pt/bitstream/10316/94718/1/Disserta%C3%A7%C3%A3o%20-%20Jos%C3%A9%20Ricardo%20Marques%20Branco%20-%20uc2012153587%20-%20pdf.pdf. Consultado em 15/01/24

CANOTILHO, J.J. Gomes / MOREIRA, Vital, 2007, *Constituição da República Portuguesa anotada: artigos 1.º a 107.º*, Vol. I, Coimbra Editora

CARDOSO, Rui, 2018, «Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15/IX», in *Revista do Ministério Público*, n.º 153, pp. 167-214

CARRAPIÇO, Helena, 2005, «O crime organizado e as novas tecnologias: uma faca de dois gumes», in *Nação e Defesa,* p. 177. Disponível em https://comum.rcaap.pt/bitstream/10400.26/1156/1/NeD111_HelenaCarrapico.pdf. Consultado em 25/03/23.

CORREIA, João Conde, 1999, «Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?» in *Revista do Ministério Público* nº 79, pp. 45-67

CORREIA, João Conde, 2014, «Prova digital: as leis que temos e a lei que devíamos ter», in *Revista do Ministério Público,* 139

COSTA, José de Faria, 1999, «As telecomunicações e a privacidade : o olhar (in)discreto de um penalista» in actas do Colóquio organizado pelo IJC em 23 de Abril de 1998, coord. António Pinto Monteiro, Coimbra: Instituto Jurídico da Comunicação

DIAS, Jorge de Figueiredo, 1974, *Direito Processual Penal*, Coimbra Editora

DIAS, Jorge Figueiredo, 1991, «Sobre o Estado Actual da Doutrina do Crime. 1ª Parte: Sobre os Fundamentos da Doutrina e a Construção do Tipo-de-Ilícito», in *Revista Portuguesa de Ciência Criminal*, ano 1, pp. 9-54

DIAS, Jorge Figueiredo, 2004, *Clássicos Jurídicos - Direito Processual Penal*, Coimbra Editora

DIAS, Figueiredo, 2008, «Sobre a Revisão de 2007 do Código de Processo Penal Português», in *Revista Portuguesa de Ciência Criminal*, ano 18, n.º 2 e 3, pp. 367-385

DRAY, Guilherme Machado, 2008, *Direitos de Personalidade: Anotações ao Código Civil (português) e ao Código do Trabalho (português)*, Almedina

FIDALGO, Sónia, 2019 (a), «A apreensão de correio eletrónico e a utilização noutro processo das mensagens apreendidas», in *Revista Portuguesa de Ciência Criminal*, n.º 29, pp. 59-74

FIDALGO, Sónia, 2019 (b), « A recolha de prova em suporte eletrónico – em particular, a apreensão de correio eletrónico» in *Julgar*, n.º 38, pp. 151-160

FREITAS, José Pedro Coutinho, 2017, *Os Meios de Obtenção de Prova Digital na Investigação Criminal: o Regime Jurídico dos Serviços de Correio Eletrónico e de Mensagens Curtas*, [Dissertação de Mestrado da Faculdade de Direito da Universidade do Minho]. Disponível em

https://repositorium.sdum.uminho.pt/bitstream/1822/64098/1/Disserta%C3%A7%C3%A3o%2BMestrado.pdf. Consultado em 23/01/24.

GONÇALVES, Fernando / ALVES, Manuel João, 2009, *A Prova do Crime: Meios Legais para a sua Obtenção*, Almedina

JESUS, Francisco Marcolino de, 2015, *Os Meios de Obtenção de Prova*, Almedina

MENDES, Paulo de Sousa, 2004, «As proibições de prova no processo penal», in *Jornadas de Direito Processual e Direitos Fundamentais*, coord. Maria Fernanda Palma, Almedina, pp. 133-154

MENDES, Paulo de Sousa / RAMALHO, David Silva, 2019, «A prova digital é o tema mais relevante em processo penal», in *Jornal Económico*. Disponível em https://www.ulisboa.pt/sites/ulisboa.pt/files/public/a_prova_digital_e_o_tema_mais.pdf. Consultado em 13/04/23.

MESQUITA, Paulo Dá, 2010, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora

MIRANDA, Jorge / MEDEIROS, Rui, 2010, Constituição Portuguesa Anotada – Tomo I, Coimbra Editora

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

NOVAIS, Jorge Reis, 2010, *As restrições aos direitos fundamentais não expressamente autorizadas pela Constituição*, Coimbra Editora

NUNES, Duarte Rodrigues 2018 (a), «Algumas reflexões em matéria apreensão de correio eletrónico e registos de comunicação de natureza semelhante» in Revista Científica sobre Cyberlaw do Centro de Investigação Jurídica do Ciberespaço, n.º VI. Disponível em https://www.academia.edu/37590489/ALGUMAS_REFLEX%C3%95ES_EM_MAT%C3%89RIA_APREENS%C3%83O_DE_CORREIO_ELETR%C3%93NICO_E_REGISTOS_DE_COMUNICA%C3%87%C3%83O_DE_NATUREZA_SEMELHANTE_1_pdf. Consultado em 18/01/24.

NUNES, Duarte Rodrigues, 2018 (b), *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal

RAMALHO, David Silva, 2017, *Métodos Ocultos de Investigação em Ambiente Digital*, Almedina

RAMOS, Armando Dias, 2014, *A prova digital em processo penal: o correio eletrónico*, Chiado Books

RODRIGUES, Benjamim Silva, 2008, *Das Escutas Telefónicas – A Monitorização dos Fluxos Informacionais e Comunicacionais – Tomo I*, Coimbra Editora

RODRIGUES, Benjamim Silva, 2009, *Das Escutas Telefónicas – Tomo II: à obtenção da prova (em ambiente) digital*, Coimbra Editora

RODRIGUES, Benjamin Silva, 2011, *Da prova penal – Tomo IV: Da prova eletrónico-digital e da criminalidade informático-digital*, Rei dos Livros

ROSA, Madalena Afra / CASANOVA, Nuno Salazar, 2021, « "Burn after reading": A apreensão de e-mails e comunicações de natureza semelhante em processo-crime e em processo contraordenacional», in Actualidad Jurídica Uría Menéndez, n.º 57. Disponível em https://www.uria.com/pt/publicaciones/7851-burn-after-reading-a-apreensao-de-emails-e-comunicacoes-de-natureza-semelhan. Consultado em 15/02/24.

SANTOS, Rita Coelho dos, 2005, «O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos», in *Boletim da Faculdade de Direito*, Coimbra Editora

VASCONCELOS, Pedro Pais de, 2006, *Direitos de Personalidade*, Almedina

VENÂNCIO, Pedro Dias, 2011, *Lei do Cibercrime Anotada e Comentada*, Coimbra Editora

VERDELHO, Pedro, 2009, «A nova Lei do Cibercrime», in *Scientia Iuridica*, LVIII

Jurisprudência

- Acórdão do Tribunal da Relação de Lisboa de 11.01.2011 (Ricardo Cardoso), processo n.º 5412/08.9TDLSB-A.L1-5, in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument

- Acórdão do Tribunal da Relação de Évora de 20.01.2015 (João Gomes de Sousa), processo n.º 684/14.6GCFAR-A.E1, in http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument

- Acórdão do Tribunal da Relação do Porto de 20.01.2016 (Artur Oliveira), processo n.º 1145/08.4PBMTS.P1, in https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/54a82f139588437f80257f5a0033e764?OpenDocument

- Acórdão do Tribunal da Relação de Evóra de 09.01.2018 (Alberto Borges), processo n.º 263/15.7T9ALR.E1, in http://www.dgsi.pt/jtre.nsf/-/8521E0E81EFC0B308025822700320074

- Acórdão do Tribunal da Relação de Lisboa de 06.02.2018 (João Carrola), processo n.º 1950/17.0T9LSB-A.L1-5, in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument

- Acórdão do Tribunal da Relação de Lisboa de 07.03.2018 (Conceição Gonçalves), processo n.º 184/12.5TELSB-B.L1-3, in https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f46dd746a7530742802583850037249e?OpenDocument

- Acórdão do Tribunal Constitucional n.º 464/2019 de 21.10.2019, processo n.º 26/2018, in https://www.tribunalconstitucional.pt/tc/acordaos/20190464.html

- Acórdão do Tribunal da Relação de Lisboa de 27.01.2021 (Rui Miguel Teixeira), processo n.º 184/12.5TELSB-R.L1-3, in https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/1beb942c43eaa700802586760032418f?OpenDocument

- Acórdão do Tribunal Constitucional n.º 687/2021 de 22.09.2021, processo n.º 830/2021, in https://diariodarepublica.pt/dr/detalhe/acordao-tribunal-constitucional/687-2021-171674458

- Acórdão do Tribunal da Relação do Porto de 08.06.2022 (José António Rodrigues da Cunha), processo n.º 293/20.7PAVFR.P1, in https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/91a806c80947fbfa802588680048e9e3?OpenDocument

- Acórdão do Tribunal da Relação de Lisboa de 15.06.2022 (Carlos Melo Marinho) processo n.º 10626/18.0T9LSB-B.L1-PICRS, in https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e4c951aeb4c729af8025888e00320fbc?OpenDocument
- Acórdão do Supremo Tribunal de Justiça de 11.10.2023 (Pedro Branquinho Dias), processo n.º 184/12.5TELSB-R.L1-A.S1 in https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/9b1e715fa7cdbceb80258a4b003f6591?OpenDocument