JOANA FILIPA MARTINS CAVACO

A APREENSÃO DE CORREIO ELETRÓNICO NO PROCESSO PENAL PORTUGUÊS:

UM ESTUDO À LUZ DO ARTIGO 17.º DA LEI DO CIBERCRIME

Dissertação com vista à obtenção

do grau de Mestre em Direito Público

Orientador:

Professor Doutor Frederico de Lacerda da Costa Pinto,

Professor da Faculdade de Direito da Universidade Nova de Lisboa

junho de 2018

JOANA FILIPA MARTINS CAVACO

A APREENSÃO DE CORREIO ELETRÓNICO NO PROCESSO PENAL PORTUGUÊS:

UM ESTUDO À LUZ DO ARTIGO 17.º DA LEI DO CIBERCRIME

Dissertação com vista à obtenção

do grau de Mestre em Direito Público

Orientador:

Professor Doutor Frederico de Lacerda da Costa Pinto,

Professor da Faculdade de Direito da Universidade Nova de Lisboa

junho de 2018

Declaração de Compromisso de Anti Plágio

Declaro por minha honra que o trabalho que apresento é original e que todas as citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, junho de 2018

Agradecimentos

Este estudo é o resultado de uma investigação, reflexão e trabalho pessoais, mas que, felizmente, pude partilhar com algumas pessoas e instituições e receber das mesmas um valioso contributo, sem o qual a chegada a este estádio jamais seria possível.

À Dilar e ao João, a quem Deus me deu a bênção de poder chamar Mãe e Pai, por todo o amor e apoio incondicional, pela presença e dedicação constantes e por me educarem nos valores da justiça, equidade e retidão, nunca me deixando perder o bom senso e que me têm auxiliado a compreender e percorrer os caminhos que conduzem ao bem.

À Avó Leonilde, pelo exemplo de uma vida de trabalho e independência e pela sabedoria e sensatez das suas palavras que me ampararam nos momentos de maior inquietação em que a distância e a ausência mais se fizeram sentir.

Ao Senhor Professor Frederico da Costa Pinto, por ter aceitado a orientação do presente estudo, pela disponibilidade e interesse demonstrados pelo meu trabalho e pela sabedoria e exigência nos comentários e sugestões que, com certeza, contribuíram para a qualidade do mesmo.

À Faculdade de Direito da Universidade Nova de Lisboa, por, há 6 anos, me ter recebido, concedendo uma excelente e irrepreensível formação e por me desafiar a ser melhor todos os dias.

A todas as minhas Professoras e Professores com os quais tive o privilégio de aprender e crescer, enquanto estudante e ser humano, ao longo de todo o meu percurso escolar e académico. Um agradecimento especial, aos que, nesta fase, demonstraram interesse pelo meu trabalho e que, de diversas maneiras, com sugestões, elementos de estudo e partilha de ideias me auxiliaram na realização do mesmo.

Aos meus colegas e amigos que comigo caminharam nesta jornada, pela compreensão dos sacrifícios que este estudo exigiu, pela partilha e esclarecimento de dúvidas e pontos de vista que aprimoraram todo o percurso de investigação, pela enorme paciência e motivação que permitiram superar os momentos em que o cansaço e a prostração pareciam querer vencer e pela sincera amizade.

Às “Farenses” que me apoiaram e me incentivaram, desde o primeiro dia, mesmo sabendo que a minha escolha implicaria sacrifícios e ausências, mas que a nossa amizade demonstrou ser capaz de superar.

À Polícia Judiciária de Faro por me ter aberto as portas, dando-me total liberdade para colocar todas as questões e por comigo partilhar os conhecimentos que só a experiência na primeira pessoa pode permitir.

À UMAC, a toda a equipa, pela oportunidade de experienciar o mundo profissional, ainda, num contexto, em parte, académico, o que potencializa as duas componentes de maior importância num bom jurista, a capacidade de ser prático sem perder o espírito académico e o gosto por aprender.

Modo de citar e outras convenções

O texto, sob recomendação e acordo do orientador, segue a seguinte forma de citar:

As monografias citadas, ao longo do texto, em nota de rodapé, têm, na primeira citação, indicação do autor, título da obra, volume ou tomo, se aplicável, em itálico, local de publicação, editora, ano e página ou páginas relevantes no contexto da citação. A partir da segunda citação, refere-se apenas o autor, o título da obra abreviado e a página ou páginas relevantes. Não são citadas várias edições de uma mesma obra.

Os artigos em publicações periódicas citados, ao longo do texto, em nota de rodapé, têm, na primeira citação, indicação do autor, título do artigo, entre aspas, título da publicação periódica, em itálico, ano, número, data e página ou páginas relevantes. A partir da segunda citação, refere-se apenas o autor, título da publicação periódica abreviado, ano, número, data e página ou páginas relevantes.

Os autores, com mais do que um apelido, são citados, a partir da segunda citação, pelo apelido pelo qual são conhecidos, *v.g.* Paulo Sousa Mendes, por Sousa Mendes, ou Frederico da Costa Pinto, por Costa Pinto.

Utiliza-se a expressão *Idem* nas citações imediatamente seguintes do mesmo autor e da mesma obra, indicando-se a página ou páginas relevantes.

Utiliza-se a expressão *Ibidem* nas citações imediatamente seguintes do mesmo autor, da mesma obra e da(s) mesma(s) página(s).

Utiliza-se o itálico para estrangeirismos e para palavras ou expressões a que se pretende dar relevo.

Nas citações mais extensas em parágrafos autónomos é também utilizado o itálico, bem como um tamanho de letra menor.

Para uma leitura mais intuitiva, evitando quebras pela utilização de algumas expressões ou conceitos, utiliza-se ocasionalmente, no texto, siglas e abreviaturas que constam da lista de abreviaturas.

A bibliografia e a jurisprudência, consultadas e citadas, constam do final do trabalho.

A presente dissertação foi redigida segundo as regras do Novo Acordo Ortográfico.

As citações diretas seguem o acordo adotado pelos respetivos autores, bem como a língua original em que foram escritas.

Para efeitos do presente estudo considerou-se a legislação, a doutrina, a jurisprudência e a documentação acessível ou com entrada em vigor até março de 2018.

Lista de abreviaturas

Al. – Alínea

Art. – Artigo

CEDH – Convenção Europeia dos Direitos do Homem

Cfr. – Confirmar/ confrontar

Coord. – Coordenação

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

Dir. – Direção

DLG – Direitos, Liberdades e Garantias

DUDH – Declaração Universal dos Direitos Humanos

Etc – et cetera

IP – Protocolo de *Internet*

JIC – Juiz de Instrução criminal

LC – Lei do Cibercrime (Lei n.º 109/2009 de 15 de setembro)

LCC – Lei do Cibercrime

MMS – Multimedia Messaging Service

MP – Ministério Público

N. º – número

NTIC – Novas Tecnologias de Informação e Comunicação

OPC – Órgão(s) de Polícia Criminal

P. – página(s)

RDI – Revista de Direito Intelectual

RMP – Revista do Ministério Público

SMS – Short Message Service

T. – Tomo

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

V.g – verbi gratia

Vol. – Volume

Declaração de Conformidade do Número de Caracteres

Declaro que o corpo da tese, incluindo espaços e notas, ocupa um total de 186.285 caracteres.

Declaro ainda que o Resumo utiliza 1.820 caracteres e o Abstract ocupa 1.781 caracteres, incluindo espaços.

Lisboa, junho de 2018

“Onde há soberba, há ignomínia, mas onde há humildade há também sabedoria.”

(Pr. 11:12)

“Não abandones a sabedoria e ela te guardará;

ama-a e ela te protegerá.”

(Pr. 4:2)

Resumo

A mensagem de correio eletrónico é um meio de prova imprescindível na investigação de determinados crimes. Nesta perspetiva, é fundamental explicar de forma clara e rigorosa o seu atual regime de obtenção, alertando para os seus principais problemas. A apreensão de mensagens de correio eletrónico encontra-se regulada no artigo 17.º da Lei do Cibercrime que, conquanto estabeleça alguns dos requisitos e pressupostos, remete para o regime de apreensão de correspondência previsto no Código de Processo Penal. As dissemelhanças técnicas e jurídicas da mensagem de correio eletrónico face à correspondência tradicional originam incongruências no sistema que acabam por traduzir-se em atribuições erradamente distintas de tutela constitucional, em decisões jurisprudenciais completamente contraditórias e em violações ou derrogações da norma sem qualquer fundamento legal. O principal foco do presente estudo é a defesa de uma interpretação que tem como ponto de partida e de chegada, por um lado, os princípios jurídico constitucionais e, por outro lado, a letra da lei, que permite uma aplicação clara e uniforme da norma, com um mínimo de correspondência verbal com o que é estabelecido pela mesma e, principalmente, uma maior previsibilidade e segurança jurídicas. São múltiplas as conclusões que podem retirar-se do presente estudo, correspondendo, no fundo, às respostas para as questões controvertidas que, aqui, serão analisadas. Pode adiantar-se que uma das grandes conclusões a que se chegou é a de que a mensagem de correio eletrónico, independentemente do seu estado, merece a tutela constitucional atribuída às comunicações, mas pelas suas especificidades carece de um regime de obtenção autónomo e específico adaptado às exigências introduzidas pela prova digital no atual sistema processual penal português.

Palavras-chave: mensagem; correio eletrónico; comunicação; correspondência; apreensão; prova; processo penal;

Abstract

Electronic mail messages are an indespensable means of evidence for the investigation of certain crimes. Therefore, it is essencial to clearly and rigorously explain its the current legal framework, pointing out its main issues. The Seizure of electronic mail messages is regulated under article 17th of the Cybercrime Law, which, while establishing some of the requirements and preassumptions, does refer to the correspondence seizure regime envisaged by the Criminal Procedure Code. The technical and legal dissimilarities of electronic mail, when compared to traditional correspondence, originate inconsistencies in the system that end up leading to the wrongful attribution of different constitutional protection, in totally contradictory jurisprudential decisions and in violation or derogation of the norm, deprived of any legal basis. The main focus of the present study is the defense of an interpretation which has both as a starting and arrival point, on the one side, the constitutional principles, and, on the other, the written law, that allows for a clear and uniform application of the norm, keeping a minimum of verbal congruity with what it establishes, and, mainly, a greater legal predictability and security. Multiple theses may be derived from the present study. Those will, after all, correspond to the answers for the controversial questions tal will, hereby, be analysed. It can be, henceforth, advanced that one of the main theses reached is that electronic mail messages, regardless of its status, requires the same constitutional tutelage which is granted to communications, but, given its specificities, lacks a particular and autonomous regime, adapted to the requests introduced by digital evidence in the current portuguese criminal procedure system.

Keywords: message; electronic mail (*E-mail*); comunication; correspondence; seizure; evidence; criminal procedure;

Introdução

O presente estudo tem por objeto o regime da apreensão de correio eletrónico no processo penal português, atualmente, consagrado no artigo 17.º da Lei do Cibercrime, com remissão para o regime da correspondência presente no artigo 179.º do Código de Processo Penal.

Com o intuito de esclarecer o conteúdo da previsão normativa do regime da apreensão de correio eletrónico, este estudo visa problematizar a remissão para o artigo 179.º do Código de Processo Penal, bem como a sua extensão. Explicitam-se os problemas com que o atual regime se depara, problemas esses que são, inclusivamente, por ele criados. Apresenta-se uma reflexão, quer sobre o impacto desta nova realidade, a prova digital, *maxime*, o correio eletrónico, quer sobre as alternativas que podem ser adotadas para suprir as atuais falhas e a atual desordem legislativa e interpretativa, salientando a importância da autonomização do seu tratamento.

A clarificação e a desmistificação das várias posições contraditórias, assumidas pela doutrina e pela jurisprudência e a advertência para as suas consequências teóricas e práticas, constituem razões que justificam o estudo deste tema.

Assim, importa explicitar a estrutura do presente estudo.

O texto encontra-se dividido em três capítulos.

O primeiro capítulo compreende um enquadramento concetual sobre a prova digital, onde se demonstra a sua relevância e se pondera sobre os novos desafios que coloca ao processo penal atual.

O segundo capítulo respeita ao correio eletrónico e às mensagens recebidas e enviadas através do mesmo, enquanto meio de prova. Introduz-se um possível conceito de correio eletrónico como meio de comunicação. Seguidamente, é apresentado um breve enquadramento jurídico-constitucional deste meio de prova. Aprecia-se a questão da equiparação do correio eletrónico à correspondência tradicional, cujos trabalhos publicados e aqui citados chegam a conclusões opostas e onde assumimos a nossa posição de destrinça e autonomia. Ainda neste segundo capítulo, apresenta-se um dos pontos com que nos deparamos, atualmente, e que mais pertinência adquire, a distinção jurisprudencial entre o correio eletrónico aberto e fechado, cujas respostas a esta questão

são altamente contraditórias, principalmente, quanto a aspetos primordiais para o processo que exigem as tão desejadas certeza e segurança jurídicas.

O terceiro capítulo é dedicado à análise do regime da apreensão de correio eletrónico enquanto meio de obtenção de prova. Inicia-se com uma breve resenha histórica, uma vez que o propósito do presente estudo não é o de fazer um ensaio histórico exaustivo do regime, mas, unicamente, uma pequena e breve contextualização até chegarmos ao regime que vigora atualmente. Na exposição do regime, levantam-se as questões consideradas pertinentes e que geram, atualmente, discórdia e alguns perigos à investigação criminal e ao próprio processo penal. Neste ponto, problematiza-se também de uma forma breve, a apreensão de correio eletrónico no telemóvel. Analisa-se, ainda, a questão atinente ao consentimento do visado e a problemática da dependência da obtenção das mensagens de correio eletrónico a este sujeito ou a quem esteja legalmente autorizado a dar acesso. Por fim, apresenta-se a nossa posição quanto à autonomização do regime da prova digital, em especial, da apreensão de correio eletrónico no processo penal português.

O objeto do presente estudo, por razões de delimitação temática e de gestão de tempo e espaço, cinge-se às mensagens de correio eletrónico. A apreensão de registos de comunicações de natureza semelhante merece um tratamento tão ou mais profundo e dedicado quanto a apreensão de mensagens de correio eletrónico, pelo que atendendo às limitações a que este estudo se encontra sujeito, optou-se por não abordar este ponto. Ainda que existam referências pontuais quanto às *SMS* ou às *MMS*, nomeadamente, nas decisões jurisprudenciais citadas e na questão da apreensão realizada através de telemóvel, tal justifica-se pela consideração das *SMS* ou das *MMS* como dados armazenados em suporte digital tal como as mensagens de correio eletrónico.

O correio eletrónico (e a mensagem) enquanto meio de prova e a sua apreensão enquanto meio de obtenção de prova relevam, não apenas no direito processual penal, mas também noutros domínios adjacentes, como o direito das contraordenações. Porém, por razões de delimitação do objeto do presente estudo, apenas serão analisados no âmbito do processo penal. Ainda que se recorra a bibliografia respeitante a disciplinas distintas do direito processual penal, nomeadamente do direito da concorrência, a sua menção restringe-se à parte que consideramos poder ser aplicada, inclusivamente por referência dos autores, ao direito processual penal.

Ainda que sejam proferidas breves explicações técnicas que se mostram importantes para a compreensão do objeto do presente estudo, a perspetiva do mesmo é, puramente, jurídica.

Conquanto se faça uma breve referência à cooperação internacional, este estudo não pretende, por questões de delimitação do objeto, abordar os problemas atinentes a esta questão, apenas se pretende demonstrar que existem mecanismos de cooperação internacionais legalmente previstos como forma de permitir o acesso a este meio de prova.

Poderia ser pertinente uma abordagem de Direito Comparado sobre o tratamento dado a este meio de obtenção de prova, tendo em conta que existe legislação internacional que determinou que vários Estados adotassem um regime de recolha e obtenção de prova no âmbito do cibercrime e pelo facto de a transposição da mesma, por estes, ter ocorrido de formas bastante distintas. Todavia, por razões de delimitação do objeto do presente estudo, optou-se por uma perspetiva, estritamente, nacional.

O intuito deste estudo não é esgotar, de maneira alguma, a análise e reflexão sobre a mensagem de correio eletrónico enquanto meio de prova e a sua apreensão enquanto meio de obtenção de prova. Pretende, sim, através de uma análise dogmática, expor as questões consideradas relevantes e apresentar a nossa posição relativamente a cada uma, incluindo, pontualmente, algumas soluções que se consideram ser adequadas.

Capítulo I – A prova digital em processo penal

1.Conceito

Em processo penal, um dos elementos fundamentais para a investigação e descoberta da verdade é a prova, através da qual se transfere para o processo a verdade histórica, permitindo realizar uma construção processual, de forma documentada e dentro do quadro de legalidade processual, do que se pode aceitar que aconteceu na realidade.

"Com a recolha de prova pretende determinar-se se alguém praticou, ou não, factos qualificados como crime. Pretende portanto apurar-se a verdade. Mas, por outro lado, descoberta a existência de culpados de um crime, a actividade probatória em processo penal tem em vista reunir elementos de prova que, reproduzidos em julgamento, permitam ao tribunal condenar aqueles culpados"[1].

Importa, ainda antes de entrar no âmbito da prova digital, fazer a distinção entre as três realidades atinentes à prova.

Primo, a prova enquanto atividade probatória que consiste no "ato ou complexo de atos que tendem a formar a convicção da entidade decisora sobre a existência ou inexistência de uma determinada situação factual"[2].

Secundo, a prova enquanto meio de prova que consiste nos "elementos com base nos quais os factos relevantes podem ser demonstrados"[3], que são "por si mesmos fonte de convencimento"[4].

Tertio, a prova enquanto resultado que consiste na "convicção da entidade decisora formada no processo sobre a existência ou não de uma dada situação de facto"[5].

Foquemo-nos na prova digital enquanto meio de prova.

A prova digital, enquanto meio de prova, "pode definir-se como qualquer informação, com valor probatório, armazenada [em repositórios electrónico-digitais de

[1] VERDELHO, Pedro – "A obtenção de prova em ambiente digital". *Revista do Ministério Público*. Ano 25. N.º 99 (julho-setembro 2004), p. 117.
[2] SILVA, Germano Marques da – *Curso de Processo Penal*. *Vol. II*. Lisboa: Verbo, 2011. p. 143.
[3] MENDES, Paulo de Sousa – *Lições De Direito Processual Penal*. Coimbra: Almedina, 2015. p. 173.
[4] ANTUNES, Maria João – *Direito Processual Penal*. Coimbra: Almedina, 2016, p. 110.
[5] MARQUES DA SILVA – *Curso de*, p. 144.

armazenamento] ou transmitida [em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital"[6].

Analisemos, então, cada um dos elementos que compõem a presente definição.

Informação corresponde ao conjunto de dados tratados que permitem formar conhecimento, isto é, aos factos que se demonstram relevantes para a produção de prova e, consequentemente, para a descoberta da verdade.

Não basta qualquer informação, exige-se que esta tenha valor probatório, ou seja, tem de ser informação com credibilidade e força probatória que permita demonstrar que algo aconteceu ou não. No fundo, que consiga, depois de esgotada a prova, formar no julgador uma convicção capaz de afastar a dúvida razoável, pertinente e impossível de resolver[7] e que através da aplicação do princípio *in dubio pro reo* garanta a efetividade da presunção de inocência[8].

Tal como se exige com a prova tradicional, a prova digital, para permitir criar no julgador uma convicção sobre os factos que fundamentam a aplicação da lei, deve superar o nível de mera informação.

Encontra-se "armazenada em repositórios electrónico-digitais de armazenamento"[9], isto é, num servidor localizado em determinado lugar, onde existe um "armazém" com discos rígidos que têm ligação à *Internet* onde é guardada toda a informação.

---

[6] RODRIGUES, Benjamim Silva – *Direito Penal Parte Especial. Tomo I. Direito Penal Informático-Digital*. Coimbra: Coimbra Editora, 2009, p. 722.

[7] Sobre a caracterização da dúvida razoável, pertinente e impossível de resolver, *vide*, PINTO, Frederico de Lacerda da Costa – *A categoria da punibilidade. Vol. II.* Coimbra: Almedina, 2013. p. 1245, nota de rodapé n.º 357 e p. 1246, "dúvida sobre os pressupostos materiais da responsabilidade penal do agente (ou seja, para todos os efeitos, sobre a existência jurídica do crime)".

[8] Neste sentido, COSTA PINTO – *A categoria,* p. 1245. "O princípio *in dubio pro reo* constitui assim uma garantia processual da efectividade da presunção de inocência do arguido e do princípio da culpa, num Estado de Direito em sentido material.
Trata-se, contudo, não de um princípio de obtenção e valoração da prova, mas antes um princípio de valoração da dúvida depois de esgotada a prova. Por isso a sua intervenção no processo decisório é subsidiária do princípio da investigação e das regras de valoração da prova. Só depois de obtida, valorada e esgotada a prova é que pode ser invocado legitimamente o princípio *in dubio pro reo*, que, por isso mesmo, não funciona como critério decisório geral, mas apenas como critério de decisão perante a dúvida razoável, pertinente e não resolúvel".

[9] RODRIGUES – *Direito Penal,* p. 722.

"Transmitida [em sistemas e redes informáticas ou redes de comunicações electrónicas, privadas ou publicamente acessíveis]"[10], ou seja, quando abrimos uma página da *Internet*, *v.g. Facebook*, estamos a conectar-nos ao seu servidor e a partir desse momento podem ser enviadas e recebidas mensagens, através dos servidores que dão autorização para que determinada mensagem saia de um dispositivo e seja enviada (em formato binário) para outro.

"Sob a forma binária ou digital"[11], por contraposição ao sistema analógico que se caracteriza por ser contínuo, é a forma de representação que ocorre nas máquinas, em que o número de estados que a máquina compreende dependerá da sua capacidade de memória. O suporte binário consiste na transformação de dados, que na natureza são contínuos, em dados discretos, limitados, que podem ser armazenados com os números 0 e 1 e será a conjugação destes dois números que dará origem a diferentes informações que podem ser armazenadas e partilhadas.

A prova digital apresenta algumas características específicas face à chamada prova tradicional, que passaremos a enunciar e que serão desenvolvidas, *infra*, no ponto respeitante às vicissitudes da sua obtenção.

Desde logo, tem um elevado grau de tecnicidade, quer quanto à informação que pode conter, quer quanto à forma de obtenção, por implicar a entrada em sistemas eletrónico-informáticos.

A facilidade de dissipação e de transformação são também características da prova digital. Num documento manuscrito ou impresso, uma alteração ou acrescento de informação será, praticamente, impossível de não ser percetível. No caso de um documento em suporte digital, por exemplo, em formato *Word*, facilmente, se consegue modificar o que aí se encontra escrito, ainda que essa modificação possa ficar registada.

Não obstante, o acesso a este tipo de prova poderá ser mais fácil, não sendo necessário, por exemplo, a deslocação ao local onde se encontra, isto é, ao local onde se encontram o servidor e os discos rígidos que guardam toda a informação, para que se possa aceder e

[10] RODRIGUES – *Direito Penal*, p. 722.
[11] *Ibidem.*

recolher, bastando o acesso ao sistema informático ou a outro a que seja permitido o acesso legítimo a partir do primeiro.

Tal como acontece com a prova tradicional, a prova digital tem de respeitar na sua admissão, obtenção e valoração todos os princípios legais e constitucionais do processo penal, presentes na Constituição da República Portuguesa (CRP) e no Código de Processo Penal (CPP), ou seja, para poder ser admitida no processo e valer como prova tem de ser uma prova legal.

Devido às suas fragilidades é essencial que se respeite o "princípio da não alteração da prova eletrónico-digital no acto de recolha, tratamento e armazenamento"[12], tendo um especial cuidado para que não sejam introduzidos ou alterados dados que possam ser prejudiciais para o processo.

Deve ainda respeitar-se, no momento da recolha da prova digital, o "princípio da documentação"[13], o que implica que "acesso, recolha, armazenamento, transferência, preservação ou apresentação/repetição"[14] devem ser sempre registados.

Em consequência do princípio da pessoalidade[15], em que cada profissional é responsável pelas provas que recolheu, surge o "princípio da responsabilização repartida dos vários intervenientes na produção da prova no respeito dos princípios forenses digitais"[16], em que cada um "deve ser responsável pela recolha, acesso, armazenamento ou transferência da prova que se encontre sob a sua alçada de investigação e custódia"[17].

Tudo isto tem por base a "manutenção da integridade, fiabilidade e valor probatório da prova digital"[18].

"A prova digital somente será válida, num dado processo penal, se forem respeitadas várias regras ao nível do acesso, recolha, armazenamento, transferência, preservação ou apresentação/repetição"[19].

---

[12] RODRIGUES – *Direito Penal,* p. 727.
[13] *Ibidem.*
[14] *Ibidem.*
[15] RODRIGUES – *Direito Penal,* p. 728.
[16] *Ibidem.*
[17] *Ibidem.*
[18] *Ibidem.*
[19] RODRIGUES – *Direito Penal,* p. 729.

2. Relevância

A rápida evolução tecnológica a que temos assistido, que corresponde, no fundo, ao surgimento e desenvolvimento das chamadas Novas Tecnologias de Informação e Comunicação (NTIC), trouxe diversas vantagens que vieram facilitar, em vários aspetos a nossa vida, mas que, em contrapartida, criaram desafios e problemas, nomeadamente à investigação criminal.

Atualmente, a utilização de meios informáticos é algo que faz parte do nosso quotidiano e a que recorremos com grande facilidade e regularidade. Em pouco tempo assistimos a uma enorme evolução dos meios tecnológicos. O acesso à *Internet* e as novas formas de comunicação vieram facilitar e acelerar o contacto entre as pessoas e a transmissão de informação.

Tais facilidade e regularidade de acesso levam a que também a criminalidade tenha começado a ser praticada através destes novos meios, pelo que a prova que existirá, nestes casos, encontrar-se-á em suporte digital, sendo esta uma das principais razões para o surgimento e importância da prova digital no processo penal.

"Cada vez mais, a investigação criminal exige, por força dos novos tempos, o recurso a elementos em suporte digital. Comprova-se ser necessário esclarecer e dotar as autoridades de novos métodos de investigação, desde que enquadrados pelo acervo constitucional e legal dos direitos à reserva da vida privada, ao sigilo das comunicações e à proteção de dados pessoais, revelando-se, assim essenciais as ideias de proporcionalidade e de ponderação relativa dos interesses em causa"[20].

"A intromissão na vida privada, no domicílio e nas telecomunicações é particularmente preocupante no ambiente digital. A informática e as ferramentas que disponibiliza multiplicam a possibilidade de invadir estas áreas reservadas dos cidadãos. Num ambiente globalizado de redes, estas potencialidades são potenciadas pela facilidade de circulação de dados"[21].

A prova digital, pelas suas características e pela sua origem, isto é, utilização de sistemas eletrónico-digitais, tem vindo a apresentar-se como uma vantagem para quem

[20] ANTUNES – *Direito Processual*, p. 29.
[21] VERDELHO – *RMP*. Ano 25. N.º 99 (julho-setembro 2004), p. 120.

utiliza estes sistemas para praticar crimes. Não obstante, lança alguns desafios a quem investiga e a quem julga.

A criminalidade moderna recorre aos meios informáticos, tendo trazido, por isso, novos desafios ao processo penal. Exige-se a realização de investigações mais complexas, onde, cada vez mais, se recorre a profissionais com formação especifica, especialistas e peritos, que permitem fazer uma análise e interpretação técnica ou científica. Sendo também de frisar que todos os profissionais que intervém no processo têm de acompanhar o progresso científico e tecnológico.

Os dispositivos eletrónico-digitais não se apresentam apenas como novos meios para a prática de crimes, como também assumem um papel importantíssimo no fornecimento de elementos de prova e até nas formas de obtenção de prova.

Um computador, por exemplo, permite a prática de crimes, contém dados que podem ser importantíssimos para a investigação e descoberta da verdade, como ainda, permite que se consiga aceder, recolher e tratar esses dados.

"Isto comporta, no campo processual, a aplicação pelo juiz não somente de ciências tradicionais, mas também de outras matérias objeto de divergência e de contínua evolução também de âmbito científico"[22], como ainda o reconhecimento e a utilização de meios de prova e meios de obtenção de prova também eles digitais com especificidades e diferenças face aos meios ditos tradicionais.

Importa, no entanto, referir que, esta exigência de conhecimentos especializados não é somente de hoje, a realização de autópsias e análises de balística como forma de poder saber o que aconteceu e como aconteceu também requer a utilização de métodos técnicos e científicos. A criminalidade moderna trouxe apenas novas exigências e requisitos acrescidos aos que já existiam.

As exigências não se verificam, somente, ao nível dos conhecimentos específicos, mas também na obtenção, conservação e admissão da própria prova digital, uma vez que têm de estar reunidas as condições necessárias a garantir o sucesso do processo.

[22] TONINI, Paolo – Direito de defesa e prova científica: novas tendências do processo penal italiano". *Revista Brasileira de Ciências Criminais*. Ano 12. N.º 48 (maio-junho 2004), p. 196 e 197.

As NTIC permitiram que fossem criadas "quer as condições propícias para o surgimento de novos tipos de criminalidade, quer os meios para o aperfeiçoamento das técnicas utilizadas na prática dos crimes ditos tradicionais. Paralelemente surgiram (ou desenvolveram-se) métodos de dissipação da prova criminal pela rede que obrigam a uma renovação constante das técnicas forenses digitais"[23].

"As actividades criminosas e as organizações internacionais do crime (máfias e outras) tornaram-se globais e informacionais"[24] tudo acontece num mundo digital, cuja conceção delimitação e identificação de agentes, tempo e espaço[25] é mais difícil.

A Convenção sobre Cibercrime[26], que pretendeu criar "uma política criminal comum, com o objectivo de proteger a sociedade do cibercrime, nomeadamente através da adopção de legislação adequada e do fomento da cooperação internacional"[27], é expressão da importância da prova digital e da necessidade que existe em regulá-la.

A ratificação e transposição da Convenção sobre o Cibercrime por Portugal, que deu origem à atual Lei n.º 109/2009, de 15 de setembro, a chamada Lei do Cibercrime (LC), refletiu a preocupação e a necessidade de criar um quadro legal específico relativamente à recolha e tratamento da prova digital.

A prova tradicional está a dar lugar à prova digital, o documento físico é, cada vez mais, substituído pelo documento em formato eletrónico-digital, a tradicional carta pela mensagem de correio eletrónico ou pela *SMS*.

A prova digital "atualmente constitui o cerne da generalidade dos nossos processos penais"[28] e, em certos casos, pode ser o único meio de prova que permite demonstrar que algo aconteceu, como aconteceu e quem praticou, ou seja, o único meio que permite formar uma convicção capaz de fundamentar uma decisão.

---

[23] RAMALHO, David Silva – "A recolha de prova penal em sistemas de computação em nuvem". *Revista de Direito Intelectual*. N.º 02 (2014), p. 125.
[24] VEIGA, Armando; RODRIGUES, Benjamim Silva – *Escutas Telefónicas. Rumo à Monotorização dos Fluxos Informacionais e Comunicações Digitais.* Coimbra: Coimbra Editora, 2007, p. 14.
[25] Sobre a noção de tempo e espaço no mundo virtual, *vide* RODRIGUES – *Direito Penal*, p. 66-70.
[26] Convenção do Conselho da Europa sobre o Cibercrime, de 23 de novembro de 2001.Aprovada pela Resolução da Assembleia da República n.º 88/2009 15 de setembro de 2009 (STE 185).
[27] Preâmbulo da Convenção sobre o Cibercrime.
[28] CORREIA, João Conde – "Prova digital: as leis que temos e a lei que devíamos ter". *Revista do Ministério Público*. Ano 35. N.º 139 (julho-setembro 2014), p. 29.

Embora se reconheça que ainda não lhe tenha sido dado o tratamento que merece, resultado do surgimento de regimes, em alguns pontos convergentes, noutros bastante divergentes ou até insuficientes, criando uma desordem e insegurança na aplicação da lei, a verdade é que a doutrina e a jurisprudência[29] têm contribuído para que exista alguma estabilidade e esclarecimento de conceitos e soluções legais.

O que significa que, "a partir do acervo prático e dogmático existente é possível construir um sistema justo que – sem medo de enfrentar as novas realidades – satisfaça, de forma equilibrada, as necessidades conflituantes em jogo"[30].

[29] Ainda que também exista divergência jurisprudencial, que cremos resultar, inevitavelmente, da desordem legislativa.
[30] CONDE CORREIA – *RMP*. Ano 35. N.º 139 (julho-setembro 2014), p. 30.

3. Inovações e limites (vicissitudes na sua obtenção)

Pela sua natureza, a recolha da prova digital, por vezes, depara-se com alguns obstáculos, exigindo, por isso, que a investigação e os métodos de recolha se adaptem, de forma a garantir a sua admissão e o seu valor probatório no processo.

Caso tal não se verifique, na pior das hipóteses, o processo poderá ter de ser arquivado, por ausência de elementos que permitam e justifiquem a continuação da investigação ou do processo.

As NTIC "vieram pôr à prova uma parte significativa da dogmática jurídica. Esse facto, conjugado com a impossibilidade de acompanhamento, por parte do legislador, da evolução tecnológica, implica que a solução destes novos problemas jurídicos tenha de ser encontrada, num primeiro momento pelo intérprete, a quem caberá procurar no direito constituído a resposta a questões para as quais este não foi pensado"[31].

"O direito processual clássico fornece ferramentas de investigação que se revelam muito úteis à obtenção de prova no ambiente digital. Ou seja, a especificidade do ambiente digital não afasta a importância que têm, para a descoberta da verdade, alguns dos meios de prova já previstos no direito processual penal clássico"[32].

Isto significa que "em certos casos, é possível o aproveitamento dos conceitos existentes e aperfeiçoados ao longo dos anos mediante uma mera adaptação dos mesmos ao mundo virtual"[33].

Todavia, existem casos em que "as constantes tentativas de subsunção da realidade virtual a normas que apenas são aplicáveis ao mundo físico resultam em verdadeiros impasses jurídicos, inultrapassáveis sem intervenções legislativas no plano nacional e supranacional e sem um processo de reinvenção conceptual e dogmática"[34].

Um dos grandes obstáculos com que a investigação e o próprio tribunal se confrontam é o elevado grau de tecnicidade que caracteriza a prova digital, o que acaba por dificultar a sua recolha e apreciação. Exigindo, por isso, que se tente, ao máximo, utilizar uma

[31] RAMALHO – *RDI*. N.º 02 (2014*)*, p. 124.
[32] VERDELHO – *RMP*. Ano 25. N.º 99 (julho-setembro 2004), p. 120.
[33] RAMALHO – *RDI*. N.º 02 (2014*)*, p. 124.
[34] *Ibidem.*

"linguagem não técnica e percetível pela generalidade das pessoas"[35], sem eliminar a "utilização de termos técnicos imprescindíveis"[36].

Em consequência da facilidade de eliminação e transformação da prova mostra-se necessário que sejam tomadas medidas de precaução para evitar que tal aconteça, garantindo que a prova que é levada para o processo é uma prova "consistente"[37], com "durabilidade"[38], existindo não só "cautela na recolha e conservação"[39], como também a "necessidade de maior celeridade na sua colheita"[40].

Relativamente a este ponto, tal justifica, por exemplo, que os órgãos de polícia criminal (OPC) devam realizar um pedido ao servidor e ao Juiz de Instrução Criminal (JIC) para bloquear o acesso ao sistema informático por parte do visado, com o fim de evitar a dissipação e eliminação da prova.[41]

Outro dos grandes desafios é a conveniência de "adequação aos padrões internacionais vigentes"[42] para que a prova possa ser admitida e recolhida além-fronteiras.

Ademais, da mesma forma que se exige uma uniformidade na produção, obtenção, admissão e valoração da prova tradicional, também na prova digital, "as regras devem ser comuns a todas as modalidades de prova digital"[43].

A sua admissão no processo, tal como acontece com a restante prova, tem de ser realizada à luz dos princípios constitucionais e processuais penais. Deve, por isso, obedecer ao princípio da legalidade, previsto no artigo 125º do CPP e ainda ao catálogo de métodos proibidos de prova previsto no artigo 126.º, do mesmo diploma legal, "sob pena de tal prova não ser admitida em tribunal ou, sendo admitida, não possuir a força

[35] RODRIGUES – *Direito Penal*, p. 724.
[36] *Ibidem.*
[37] *Ibidem.*
[38] *Ibidem.*
[39] *Ibidem.*
[40] *Ibidem.*
[41] No caso da apreensão de correio eletrónico, o que se verifica, na prática, é um pedido, por parte dos OPC que procedem à diligência, para que o acesso, pelo seu titular e visado pela apreensão, seja bloqueado, nomeadamente através da alteração da palavra passe, impedindo que este elimine mensagens que se possam mostrar de grande relevância para o processo.
[42] RODRIGUES – *Direito Penal*, p. 724.
[43] *Ibidem.*

probatória exigível para perturbar a presunção de inocência do arguido criminoso informático-digital ou ciber criminoso"[44].

"Quanto ao texto constitucional, neste âmbito, destaca-se o artigo 32.º, que prevê, a este propósito, a nulidade da prova obtida mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na visa privada, no domicílio, na correspondência ou nas telecomunicações"[45]. É também de frisar o artigo 34º da CRP que consagra a inviolabilidade do domicílio e da correspondência.

A garantia dos direitos fundamentais dos cidadãos exige que a utilização das NTIC e a obtenção da prova digital ocorram sempre dentro de um quadro garantístico dos direitos, liberdades e garantias (DLG), presente tanto na CRP como no CPP.

A recolha da prova digital recorre aos meios de prova e aos meios de obtenção de prova ditos tradicionais como exames, perícias e apreensões, cujos regimes foram criados numa época em que a prova digital não era ainda equacionada. Em consequências, os princípios e os requisitos legais têm cumpridos, mas, por vezes, a sua obtenção confronta-se com impossibilidades técnicas, que podem, numa situação de extremo, inviabilizar a investigação e o processo.

A prova pericial, "apesar de ser um meio de prova clássico, é um dos instrumentos que merece mais atenção nas investigações criminais"[46]. "No ambiente informático e das redes de comunicações, as perícias são particularmente importantes, numa dupla perspetiva"[47]. Por um lado, "a opinião dos técnicos e dos peritos permite a quem investiga perceber os factos em investigação e vir assim a descobrir os repectivos autores"[48]. Por outro, "facilita a produção de prova e a perceção desses mesmos factos em julgamento"[49].

Os exames são também um meio de obtenção de prova útil "quando os vestígios não são de tal forma complexos que exijam a formalidade da realização de uma perícia. Mas têm ainda mais relevo quando, pela natureza dos factos em investigação ou pela

[44] RODRIGUES – *Direito Penal,* p. 724.
[45] VERDELHO – *RMP*. Ano 25. N.º 99 (julho-setembro 2004), p. 118.
[46] *Idem*, p. 120.
[47] *Ibidem*.
[48] *Ibidem*.
[49] *Idem*, p. 120 e 121.

especificidade dos elementos de prova recolhidos, não se torna possível realizar uma perícia"[50].

Ainda quanto aos meios de obtenção de prova, "não pode esquecer-se também a importância das buscas e apreensões, como formas essenciais para garantir a obtenção de elementos de prova"[51].

Os regimes jurídicos previstos na lei têm o intuito de permitir que a recolha de prova se faça de uma forma legal, acessível, segura e eficaz. Ora, por vezes, tal pode ser mais difícil quando entramos no domínio da prova digital, ainda que esta tenha também de ser obtida e integrada no processo.

Quando falamos em obtenção de prova tradicional, normalmente, referimo-nos, ao acesso a objetos, dados, *etc*, do visado. Na obtenção de prova digital pode mostrar-se necessário aceder também aos equipamentos e dados dos servidores e operadoras de comunicações. Torna-se, por isso, necessário não só a permissão de acesso a esses equipamentos e dados, como ainda que estas entidades colaborem com as autoridades policiais e judiciárias na investigação, relativamente ao acesso, recolha e conservação dos dados informáticos que se demonstrem relevantes para a investigação.

Relacionada com colaboração dos servidores e operadoras de comunicação está a cooperação internacional entre as várias entidades. Estando em causa uma prova não física, a prova digital pode localizar-se em qualquer parte do mundo, pelo que é indispensável estabelecer relações de cooperação e intercâmbio entre as entidades dos países com conexão com a prática do crime.

Por vezes, esta cooperação apresenta algumas limitações ou não existe, de todo, o que acaba por inviabilizar o acesso à prova e, por conseguinte, a boa prossecução do processo.[52]

[50] VERDELHO – *RMP*. Ano 25. N.º 99 (julho-setembro 2004), p. 121.
[51] *Ibidem*.
[52] Sobre esta questão, coloca-se o problema da dependência da autorização do servidor para poder aceder ao correio eletrónico, quando não há autorização do visado. Sendo necessário pedir ao servidor o acesso, o que se verifica é que o servidor não sendo obrigado a dar acesso, tem o poder "discricionário" de decidir as situações em que dá ou não acesso. O acesso acaba só por ser facultado quando estão em causa crimes mais graves, criminalidade altamente organizada, terrorismo, *etc*.

No mundo virtual é, extremamente, difícil ter a certeza de quem está "do outro lado" e, em consequência, saber quem é o verdadeiro agente e autor do facto. Este anonimato, pode impedir a identificação do autor ou, *inclusive*, levar a uma identificação errada.

Outro aspeto que importa referir quanto à obtenção da prova, respeita à "transparência" da obtenção e conservação da prova por parte dos OPC.

"Com efeito, continua-se a verificar-se uma tendencial opacidade da investigação criminal em ambiente digital no ordenamento jurídico português que se manifesta, desde logo, na dificuldade de o arguido ou o defensor saberem se os procedimentos, cada vez mais exigentes, de investigação criminal e subsequente recolha de prova digital são executados pelos órgãos de policia criminal na sua atividade investigatória, em termos compatíveis com os requisitos legais e as normas técnicas adequadas e relevantes, ou mesmo em que termos tais procedimentos são impostos internamente. A genérica ausência de divulgação dos procedimentos forenses utilizados em sede de investigação criminal impede uma sindicância da idoneidade dos métodos utilizados, bem como um controlo da fidedignidade da prova recolhida"[53].

"O constante progresso científico reclama uma atuação constante do legislador. É necessário que ele adeque o direito processual penal às novas realidades disponibilizadas pelo contínuo progresso científico e logo utilizadas pela criminalidade"[54].

É cada vez mais difícil para o direito, e, em particular, para o processo penal acompanhar o progresso tecnológico. A solução jurídica adotada é, rapidamente, ultrapassada, ficando desatualizada ou até inutilizada. Esta realidade pode levar à criação de espaços vazios, onde o direito não consegue chegar, nem consegue acompanhar, o que, por sua vez, pode originar um aumento de comportamentos de risco e de situações de impunibilidade que colocam em causa a segurança e os direitos dos cidadãos.

Não obstante, as dificuldades que as NTIC trouxeram à investigação, não podemos olvidar que também vieram permitir a criação de novos métodos de investigação e facilitar o acesso à prova. Se com apenas um "clique" se pode praticar um crime, também com apenas um "clique" se consegue obter informações, cujo acesso, antes, seria muito mais complicado e restrito, implicando, por vezes, uma deslocação física ao local onde essa informação se encontrava.

[53] RAMALHO – *RDI*. N.º 02 (2014), p. 156 e 157.
[54] CONDE CORREIA – *RMP*. Ano 35. N.º 139 (julho-setembro 2014), p. 53.

Destarte, se, por um lado, as NTIC trouxeram novos riscos, novos tipos de criminalidade, novos meios de prova, gerando novas exigências ao processo penal, por outro lado, em muito têm contribuído para a investigação criminal.

Capítulo II – O correio eletrónico

1. Conceito

Concluído o enquadramento do tema no que à prova digital diz respeito, passaremos para a análise do correio eletrónico enquanto meio de prova.

Importa, por essa razão, tecer alguns esclarecimentos e considerações sobre o conceito de correio eletrónico para efeitos do processo penal.

Embora, num primeiro momento, se possa pensar que a definição de correio eletrónico não apresenta grande relevância, à medida que se aprofundam conhecimentos sobre o regime da sua apreensão, tal definição mostra-se essencial para tomar uma posição relativamente à solução jurídica que consideramos ser a mais adequada.

Coloca-se, portanto, a questão de saber se o correio eletrónico, do ponto de vista do processo penal, deve ser entendido como uma forma de correspondência dentro dos parâmetros da correspondência tradicional ou como um meio eletrónico de comunicação enquadrado dentro do âmbito da prova digital.

O correio eletrónico consiste num instrumento de comunicação à distância que permite que duas ou mais pessoas que se encontram em locais diferentes e distantes possam trocar informação através do envio e receção de mensagens com a possibilidade de anexar ficheiros, bastando, apenas o acesso a um sistema informático, com ligação à *Internet* ou *Intranet*[55].

"Esta forma de comunicar, além de possibilitar uma ligação rápida, fácil, económica e capaz de enviar e receber dados informáticos, quebra todas as barreiras geográficas existentes entre o emissor e o(s) receptor(es), sem que para tal tenha havido qualquer tipo de deslocação ou prejuízo pessoal."[56]

[55] Rede de computador privada. Embora o processo técnico seja diferente, porque não há, efetivamente, um servidor de correio eletrónico, do ponto de vista material é idêntico, corresponde, no fundo, a uma comunicação, a uma transmissão de informação.

[56] ANTUNES, André Francisco Dias – "Recolha de prova digital – correio electrónico e processo penal: regimes aplicáveis e actuação dos órgãos de polícia criminal". Chambel, Élia Marina; Valente, Manuel Guedes; Santo, Paula do Espírito (Coord.) – *Ciências policiais: Estado, segurança e sociedade*. Coimbra: Almedina, 2011, p. 11.

Na Diretiva n.º 2002/58/CE[57], o artigo 2º, alínea h), define correio eletrónico como "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".

Desta definição resulta que a mensagem pode ser de texto, som ou imagem. Quanto a este primeiro elemento que compõe a definição, "mensagem textual, vocal, sonora ou gráfica", podem levantar-se algumas questões quanto à proteção da mensagem consoante a forma em causa.

Estamos perante um direito fundamental, o direito à palavra, que apresenta diferentes dimensões e proteções consoante se trate da palavra falada em tempo real, cuja proteção é mais intensa, ou da palavra escrita, que acaba por ter uma proteção menos intensa[58].

A mensagem de correio eletrónio inclui dados de base[59], de conteúdo[60] e de tráfego[61].

Uma vez recebida e conhecida pelo destinatário, a mensagem pode ser armazenada, quer no servidor, isto é, na rede, quer no próprio equipamento do destinatário, *v.g.* no computador.

Sobre o local de armazenamento da mensagem também se levantam algumas questões, nomeadamente quanto à distinção entre a utilização de um programa informático de correspondência eletrónica, como o *Outlook* e a utilização do *WebMail*.

Quanto a esta questão faremos apenas uma pequena abordagem, uma vez que consideramos que, embora se encontrem em locais diferentes, não deixam de merecer a tutela atribuída às comunicações e, por essa razão, não existe um verdadeiro problema.

Está em causa o acesso a uma conta de correio eletrónico quando realizado através de um programa informático instalado no dispositivo do recetor em que as mensagens se encontram armazenadas no sistema informático desse mesmo dispositivo e o acesso

[57] Diretiva n.º 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002.
[58] Quanto à questão da diferença entre a palavra falada e a palavra escrita *vide, infra,* ponto 2.3 do presente capítulo.
[59] Dados de identificação do utilizador, por exemplo, o Protocolo de *Internet* (IP) do computador.
[60] Inclui o texto e os ficheiros em anexo.
[61] Compostos pelos cabeçalhos técnicos da mensagem.

realizado através do *WebMail* em que as mensagens se encontram armazenadas no servidor do fornecedor do serviço e não no próprio dispositivo do visado.

Quando se realiza a apreensão do dispositivo, vulgarmente o computador, e a consequente apreensão das mensagens de correio eletrónico, se existir um programa informático instalado no dispositivo que permita o livre acesso ao correio, poderá considerar-se não ser necessária a aplicação do regime de apreensão de correspondência, uma vez que não se trata, já, de correspondência, mas sim de dados informáticos armazenados no próprio dispositivo, pelo que aplicar-se-ão os artigos 15.º e 16.º da LC relativamente à pesquisa e apreensão de dados informáticos, respetivamente.

Quando a apreensão das mensagens de correio eletrónico é realizada através do *WebMail*, deparamo-nos com algumas exigências, como a necessidade de consentimento do visado ou a autorização por parte do servidor[62] e uma vez que as mensagens não se encontram armazenadas no sistema informático do dispositivo do recetor, mas sim no sistema informático da empresa que fornece o serviço de correio eletrónio, não poderão ser consideradas como dados informáticos do destinatário e como tal livremente acessíveis.

"Enquanto os e-mails de quem utiliza contas POP3 (programas informáticos específicos para descarregar as mensagens de correio eletrónico, tais como o "OUTLOOK") ficam guardados no dispositivo eletrónico, os e-mails de quem utiliza webmail (como o "GMAIL" ou o "HOTMAIL") não são armazenados no computador, mas na "nuvem"." [63]

Contudo, tal distinção não nos parece fazer sentido. Em primeiro lugar, por considerarmos, como já referimos, que se trata, em ambos os casos, de comunicação, ou de conteúdo dela resultante, que merece a tutela do sigilo das comunicações presente na CRP, que iremos abordar *infra*.

[62] Para que quem pratica realiza a diligência possa aceder de forma legal ao sistema informático. Sobre a questão do consentimento do visado, *vide*, *infra*, ponto 2., do capítulo III.
[63] PINTO, Ângela – "Crime de abuso sexual de menores com recurso à internet: enquadramento jurídico, prática e gestão processual". Pereira, Luís Silva; Albuquerque, José Ribeiro de; Duarte, Jorge Manuel Vaz Monteiro Dias (Coord.) – *Trabalhos Temáticos de Direito e Processo Penal – Volume I*. Lisboa: Centro de Estudos Judiciários, 2016, p. 130, nota de rodapé 41.

Em segundo lugar, porque consideramos que não é o local onde se encontra a mensagem que é decisivo para determinar se é comunicação ou não, mas sim, o próprio ato comunicacional que existe ou existiu e que deu origem a determinada mensagem, com um determinado conteúdo, que merece especial tutela.

A mensagem é "enviada através de uma rede pública de comunicações"[64], ou seja, enviada por meio de um servidor que permite que determinada mensagem saia de um dispositivo e seja enviado para outro.

Pode armazenar-se em rede, ou seja, no já referido repositório eletrónico-digital, no próprio "equipamento terminal do destinatário até o destinatário a recolher"[65], isto é, no dispositivo recetor da mensagem.

"Por consiguiente, y a los solos efectos penales, por mensaje de correo electrónico puede entenderse una modalidad de comunicación, por lo general de carácter personal, que incorpora texto, voz, sonido o imagen y que se sirve de las redes telemáticas como tecnología de transmisión y de los sistemas informáticos (ordenadores y el software o sistema lógico correspondiente) como instrumentos de remisión y de recepción entre dos o más comunicantes y, en su caso, de almacenamiento de los mensajes"[66].

Na Lei n.º 41/2004[67] não se incluiu no seu artigo 2.º, com a epígrafe "Definições", a definição de correio eletrónico presente na Diretiva n.º 2002/58/CE.

Na Lei n.º 32/2008[68], também não existe qualquer definição de correio eletrónico.

Na LC, embora se regule a apreensão e a interseção de correio eletrónico, também não se estabelece uma definição de correio eletrónico.

[64] Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002.
[65] Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002.
[66] CASABONA, Carlos Maria Romeo – "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet". *Derecho y conocimiento: vol. II*. 2006. Huelva. Universidad de Huelva: Facultad de Derecho, p. 129.
[67] Lei n.º 41/2004, de 18 de agosto.
[68] Lei n.º 32/2008, de 17 de julho.
Sobre a vigência da presente lei, colocam-se algumas dúvidas, uma vez que a Diretiva que esta transpõe foi declarada inválida com efeitos desde a sua entrada em vigor. Todavia, o legislador nacional, ainda não tomou qualquer posição. O contexto de referência à presente lei é independente da sua vigência, apenas se pretende demonstrar a ausência de uma definição de correio eletrónico na legislação nacional.

Esta ausência na lei pode criar alguma confusão concetual gerada pela forte componente técnica que exige conhecimentos que, muitas vezes, os profissionais que têm contacto com este meio de prova não têm.

Não obstante a ausência de um conceito na legislação portuguesa, a doutrina tem contribuído para uma clarificação do que se pode entender como correio eletrónico.

O correio eletrónico pode ser, assim, entendido como um "fluxo informacional e comunicacional digital, sob o formato de texto, som, imagem ou gráfico, que é colocado por um assinante ou consumidor de redes ou serviços de comunicações electrónicas acessíveis ao público, no âmbito de um ciclo informacional e comunicacional (tendencialmente) fechado, através de um ponto terminal da rede, na rede pública de comunicações electrónicas ou no terminal do destinatário do fluxo até que o mesmo proceda à sua recolha, leitura, e/ou posterior eliminação"[69].

Esta nova forma de comunicação, tornou possível uma troca de informação mais rápida e económica e, por todas as vantagens que apresenta, substituiu, de uma forma quase total, a correspondência dita tradicional.

"O correio electrónico singulariza uma concreta forma de comunicação electrónica. Esse carácter electrónico dos e-mails em muito particulariza a sua definição. Torna-se assim, como facilmente se infere, incontornável a remissão para o conceito de comunicação electrónica."[70].

O envio de uma mensagem consiste numa "transferência de dados pessoais, sendo consideráveis os riscos de ocorrência de desvios, … Uma mensagem escrita em linguagem corrente, sem criptografia, pode ser lida por numerosos intermediários, se assim o desejarem. O correio electrónico utiliza um caminho tecnicamente complexo antes de atingir o seu destinatário, uma vez que circula na rede efectuando "saltos" de servidor em servidor. Pode, portanto, ser facilmente interceptado por numerosos leitores (…). Existe pois uma potencialidade, efetiva de espionagem dos endereços que assim circulam na rede"[71].

[69] VEIGA; RODRIGUES– *Escutas Telefónicas*, p. 374.
[70] ANTUNES – *Ciências policiais*, p. 11.
[71] MARQUES, José Augusto Garcia; MARTINS, António Gomes Lourenço - *Direito da informática*. 2.ª ed. Coimbra: Coimbra Editora, 2006, p. 433.

O envio da mensagem está, portanto, dependente da intervenção de um terceiro, de um prestador de serviço de comunicações eletrónicas. Deste modo, ainda que seja uma forma de comunicação privada, a confidencialidade pode ficar, de certo modo, limitada ou diminuída aquando da intervenção deste terceiro que recebe o pedido de envio, autoriza e providencia o envio da mesma ao recetor.[72]

Do ponto de vista legal não se tenha se estabeleceu uma definição, mas assumiu-se, sem qualquer dúvida, a possibilidade de utilização das mensagens de correio eletrónico como meio de prova no processo penal. "Isto é, reconhecendo que as mensagens de correio electrónico podem revelar-se importantes fontes de material probatório, a lei aceita que possam ser usadas com essa finalidade"[73].

[72] Cfr. ANDRADE, Manuel da Costa – "*Bruscamente no Verão Passado", a reforma do Código de Processo Penal: observações críticas sobre uma lei que podia e devia ser sido diferente*. Coimbra: Coimbra Editora, 2009, p. 158.
[73] VERDELHO, Pedro – "Apreensão de correio electrónico em Processo Penal". *Revista do Ministério Público*. Ano 25. N.º 100 (outubro/dezembro 2004), p. 154.

2. Enquadramento jurídico constitucional

2.1. A correspondência e os demais meios de comunicação na Constituição

Ao longo do tempo o campo de intervenção da lei fundamental no direito processual penal tem vindo a aumentar, aparecem novos princípios, reformulam-se os já existentes, permitindo dar continuidade à estreita relação que ambos mantêm.

"Em termos práticos, isso traduz-se no alargamento do direito constitucional processual penal"[74].

O artigo 32.º da CRP contém o que a doutrina denomina por c*onstituição processual penal*, consagrando um conjunto de princípios que funcionam como garantias de defesa no processo penal.

Como primeiros e últimos limites do processo temos os princípios da dignidade da pessoa humana e do Estado de Direito democrático, presentes nos artigos 1.º e 2.º da CRP.

É notória a preocupação com a proteção da correspondência. Tratando-se de uma troca de informação privada, visou-se proteger o seu sigilo e, ainda, a privacidade associada à informação que é transmitida. Por essa razão, consagrou-se, nos artigos 32.º, n.º 8 e 34.º da CRP, o sigilo da correspondência como direito fundamental[75].

O sigilo e a não ingerência na correspondência e nos demais meios de comunicação, enquanto direitos fundamentais, surgem como "*liberdades*, esferas de autonomia dos indivíduos em face do poder do Estado, a quem se exige que se abstenha, quanto possível de se intrometer"[76] e que se encontram positivadas na Constituição[77].

Na Constituição de 1933 encontrávamos, no n.º 6 do artigo 8.º, a consagração da inviolabilidade do domicílio e o sigilo da correspondência como direitos dos cidadãos, prevendo-se que a sua regulamentação deveria constar em legislação ordinária.

---

[74] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital — *Constituição da República Portuguesa Anotada: Vol. I.* 4.ª Ed. Revista. Reimpressão. Coimbra: Coimbra Editora, 2006, p. 515.
[75] Como veremos *infra*, o facto de ser um direito fundamental não significa que seja ilimitado *tout court*.
[76] ANDRADE, José Carlos Vieira de – *Os Direitos Fundamentais na Constituição Portuguesa de 1976.* 5.ª edição. Coimbra: Almedina, 2012, p. 51.
[77] GOUVEIA, Jorge Bacelar – *Manual de Direito Constitucional. Vol. II.* 6.ª ed. Coimbra: Almedina, 2016, p. 930.

A CRP de 1976 estabeleceu desde o seu início, no artigo 34.º, o sigilo e a proibição da ingerência na correspondência.

Com a Revisão Constitucional de 1997 foi acrescentada ao n.º 4 do mesmo artigo a expressão "e nos demais meios de comunicação", o que veio alargar o âmbito de aplicação desta proteção a outras formas de comunicação, nomeadamente o correio eletrónico, as conversas telefónicas, as *SMS* e as *MMS*. Isto significa que, independentemente do entendimento de correio eletrónico como forma de correspondência equiparada à correspondência tradicional ou como meio de comunicação eletrónico, este estará sempre protegido ao abrigo deste preceito.[78]

Na *constituição processual penal*, presente no artigo 32.º da CRP, o seu n.º 8 determina a nulidade das provas que tenham sido obtidas sem respeitar o artigo 34.º da CRP e os regimes da nulidade e dos métodos de obtenção de prova em causa presentes no CPP.

Estabelece-se, ainda, a nulidade e proibição de prova, no n.º 3 do artigo 126.º do CPP, quando existe obtenção de prova "mediante intromissão na correspondência ou nas telecomunicações, sem o consentimento do respectivo titular", salvaguardando as exceções previstas na lei.

Como forma de reforçar a garantia constitucional deste direito tipificou-se o crime de violação da correspondência e das telecomunicações, no artigo 194.º do Código Penal (CP).

A qualificação do sigilo da correspondência como direito fundamental tem como objetivo "limitar na maior medida possível a possibilidade de restrições, sujeitando-se estas a pressupostos bastante vinculados"[79].

Não obstante esta proteção, a CRP prevê, no n.º 4 do artigo 34.º, uma exceção que permite que, em matéria penal, as autoridades públicas possam intervir "na correspondência, nas telecomunicações e nos demais meios de comunicação"[80]. Existe,

[78] Neste sentido, TRP – Acórdão de 21 de fevereiro de 2018, processo n.º 17448/17.4T8PRT.P1. "No âmbito normativo do citado artigo 34.º inclui-se o chamado correio electrónico, porque o segredo da correspondência abrange seguramente as correspondências mantidas por via das telecomunicações. O envio de mensagens electrónicas de pessoa a pessoa (e-mail) preenche os pressupostos da correspondência privada – cfr. GOMES CANOTILHO e VITAL MOREIRA, op. cit., p. 544".
[79] GOMES CANOTILHO; VITAL MOREIRA — *Constituição*, p. 540.
[80] Artigo 34.º n.º 4 da CRP.

portanto, uma autorização constitucional expressa para a restrição, de forma ponderada e proporcional, deste direito fundamental.[81]

Isto significa que a apreensão de correio eletrónico corresponde a uma restrição de direitos fundamentais, ainda que seja uma restrição[82] mínima, cujos limites estão, expressamente, previstos na CRP, através da, chamada, habilitação legal expressa.

Devem respeitar-se os princípios da legalidade e da reserva de lei, pelo que as limitações devem estar expressamente previstas na lei, nomeadamente quanto ao correio eletrónico, no CPP e na LC, respeitando e restringindo-se sempre apenas ao que é permitido pela CRP.

Estas restrições estão sujeitas ao princípio da proporcionalidade, presente no artigo 18.º da CRP, nas suas 3 aceções, necessidade, adequação e proporcionalidade em sentido estrito. "Exige-se, uma apreciação rigorosa quanto ao princípio da proporcionalidade,

[81] TRP – Acórdão de 22 de maio de 2013, processo n.º 74/07.3PASTS.P1: "Desde logo, ninguém dirá, hoje, que os direitos fundamentais, mesmo os direitos, liberdades e garantias, são absolutos, ilimitados. "Não o são na sua dimensão subjectiva, porque os preceitos constitucionais não remetem para o arbítrio do titular a determinação do âmbito e do grau de satisfação do respetivo interesse, e também porque é inevitável e sistémica a conflitualidade dos direitos de cada um com os direitos dos outros". "Não o são também enquanto valores constitucionais, visto que a comunidade não se limita a reconhecer o valor da liberdade: liga os direitos a uma ideia de responsabilidade social e integra-os no conjunto dos valores comunitários. Assim, além dos limites «internos» do subsistema jusfundamental, que resultam das situações de conflito entre os diferentes valores que representam a s diversas facetas da dignidade humana, os direitos fundamentais têm também limites «externos», pois hão-de conciliar as suas naturais exigências com as imposições próprias da vida em sociedade: a ordem pública, a ética ou moral social, a autoridade do Estado, a segurança nacional, entre outros" ([23]) É a propósito da necessidade de superação desta tensão dialética que se fala do princípio da harmonização ou da concordância prática ([24]), como se fala ainda do princípio da proporcionalidade ([25]) ([26]). Procurando descer ao caso concreto. O artigo 32.º da Constituição da República, depois de consagrar (nº1) uma cláusula geral de garantias de defesa, preceituando que "O processo criminal assegura todas as garantias de defesa, incluindo o recurso", estabelece no seu n.º 8, no que concerne ao regime da prova proibida, que "São nulas todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações".
Do que logo decorre uma diferenciação entre a absoluta interdição da tortura, coacção, ofensa da integridade física ou moral da pessoa e a relativa interdição na intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações. Dizer, então: «a garantia constitucional de defesa no âmbito da privacidade apenas incide quando essa intrusão ou ingerência se revelarem abusivas. Não o sendo será a mesma constitucionalmente aceitável desde que tal intromissão se mostre proporcional entre a observância dos direitos, liberdades e garantias em geral (18.º, n.º 2 Constituição), tanto do agente, como da vítima, e o exercício da acção penal, no âmbito de um processo justo (20.º, n.º 1 e 4; 219.º, n.º 1 Constituição), atenta uma das finalidades primaciais do processo penal, que consiste na restauração da paz jurídica comunitária, a qual foi quebrada com a prática criminosa. Tal sucederá quando essa interferência se mostre idónea ou adequada (i), necessária ou exigível (ii), no sentido da optimização relativa do que é factualmente possível, e tudo isto na sua justa medida (iii), que diz respeito à respectiva optimização normativa".
[82] autorizada.

devendo a restrição limitar-se ao estritamente necessário à protecção de direitos e bens constitucionais e à prossecução do interesse subjacente à acção penal"[83].

Cumpre, portanto, determinar se as restrições, relativamente às comunicações eletrónicas, estabelecidas pela lei em matéria criminal, nos termos, atualmente, previstos satisfazem os requisitos do n.º 2 e do n.º 3 do artigo 18.º da CRP.

Numa primeira abordagem, diríamos que a resposta deve ser afirmativa tendo em conta, as circunstâncias da criminalidade moderna e o *modus operandi* dos seus agentes, estas restrições não violam os limites do princípio da proporcionalidade estabelecidos no artigo 18.º da CRP.

2.2. O direito fundamental à reserva da intimidade da vida privada

A matéria respeitante à correspondência e ao seu sigilo encontra-se também inserida no âmbito do direito à reserva fundamental da vida privada, presente no artigo 26.º, n.º 1, da CRP.

Também aqui se deve verificar um equilíbrio relativamente a este direito que está, intimamente, ligado aos princípios da dignidade da pessoa humana e da tutela efetiva da justiça, presentes nos artigos 1.º e 20.º, da CRP, respetivamente.

Por esta razão, independentemente de se considerar que a apreensão de mensagens de correio eletrónico, em que o ato comunicacional, em sentido estrito, já cessou, merece ou não a tutela do sigilo das comunicações, estaremos sempre perante o perigo ou a ofensa a direitos fundamentais que merecem uma tutela adequada, nomeadamente do direito à reserva da intimidade da vida privada.[84]

Tratando-se de um direito fundamental, as limitações e restrições ao exercício deste direito devem ser encaradas como exceções.

Atentemos, ainda, no artigo 29.º da Declaração Universal dos Direitos Humanos (DUDH) que estabelece que tais restrições têm de estar, legalmente, previstas,

[83] GOMES CANOTILHO; VITAL MOREIRA — *Constituição,* p. 543.
[84] Neste sentido, CARDOSO, Rui - "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX". *Revista do Ministério Público*. Ano 39. N.º 153 (jan -mar 2018), p. 178.

respeitando, sempre, os direitos e liberdades dos outros, "a fim de satisfazer as justas exigências da moral, da ordem pública e bem-estar da sociedade democrática"[85].[86]

2.3. A proteção da palavra falada e da palavra escrita

Como referimos a propósito do conceito de correio eletrónico, o facto de a mensagem poder adquirir a forma de texto, de voz, som ou imagem, poderá levantar algumas questões quanto à proteção constitucional, nomeadamente quanto ao grau de proteção conferido às mesmas, consoante a forma que esteja em causa.

A palavra falada em tempo real tem uma proteção muito intensa devido ao facto de não existir uma intenção e perceção de perpetuação no tempo como existe na palavra escrita.

Poderia colocar-se a questão se deveria atribuir-se à mensagem vocal ou sonora a proteção conferida à palavra falada em tempo real, no entanto, tal não se justifica uma vez que a forma como é transmitida, através de um programa em que a mensagem é gravada e enviada, leva-nos a crer que a proteção que lhe é devida é a da palavra escrita.

Ainda que se trate da palavra "falada", não é a palavra falada em tempo real pelo que consideramos que existe uma perceção de perpetuação no tempo. A mensagem de voz é gravada e é essa gravação que é transmitida ao destinatário.

Tem-se alertado para a existência de dificuldades práticas na investigação se tal distinção existisse. "Na verdade, imagine-se que, tendo por base os graus distintos de protecção, os órgãos competentes, munidos apenas de autorização judiciária, apreendem correio electrónico armazenado numa conta de e-mail, encontrado mensagens que anexam ficheiros de voz"[87].

Tendo em consideração a noção de correio eletrónico presente na Diretiva n.º 2002/58/CE, de 12 de julho de 2002, que inclui mensagem de voz, não cremos que se

[85] Artigo 29.º da DUDH.
[86] Importa referir a parte do artigo 29.º que se refere à de satisfação das justas exigências da moral, da ordem pública e do bem-estar de uma sociedade democrática pode configurar-se como uma perigosa cláusula aberta.
[87] NEVES, Rita Castanheira – *As ingerências nas comunicações eletrónicas em processo penal.* Coimbra: Coimbra Editora, 2011, p. 178.

possa considerar como uma conversação em tempo real, mantendo a sua natureza de comunicação eletrónica.[88]

Deste modo, não faz qualquer sentido distinguir a proteção atribuída a uma mensagem de correio eletrónico textual e "vocal", nem tão pouco se deve "equiparar" esta última às conversações telefónicas em tempo real.

No âmbito de uma conversa telefónica em tempo real, "a palavra falada é proferida naquele momento, com o já mencionado sentido de vaporização"[89], pelo que, por não existir a intenção e perceção de perpetuação da informação, exige-se uma maior proteção.

Pelo contrário, a "palavra registada com o propósito de ser enviada por correio electrónico leva já em si o mesmo grau de ponderação que conferimos à palavra escrita, enquanto acto perpetuador de uma especifica mensagem que se sabe que permanecerá para além do acto em que chega ao destinatário da comunicação"[90].

Assim sendo, conclui-se que o correio eletrónico ainda que contenha uma mensagem vocal ou sonora não merecerá a proteção da palavra falada em tempo real.

Também o CPP atribuiu uma maior proteção à palavra falada em tempo real, "como resulta do facto de que a apreensão de documento ser um meio de obtenção de prova admissível em relação a quaisquer crimes e a intercepção de conversações telefónicas ser um meio de obtenção de prova admissível em relação a um catálogo de crimes"[91].

2.4. Conclusões

A Constituição deve ser o local de consagração dos direitos fundamentais e também da sua delimitação, devendo estabelecer, de forma clara, os limites ao seu conteúdo, de modo a não deixar espaço a interpretações extensivas discricionárias que possam afetar todo o seu conteúdo.

---

[88] Cfr. NEVES – *As ingerências,* p. 178. Exceto se estiver em causa a interceção dessa mensagem em tempo real, por via do art.18.º da LC.
[89] *Ibidem*.
[90] *Ibidem.*
[91] ALBUQUERQUE, Paulo Pinto de – *Comentário do Código Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem.* 4ª Ed. Atualizada. Lisboa: Universidade Católica, 2011, p. 542.

Não devemos, contudo, afastar a ideia de que é necessária uma interpretação dinâmica dos direitos fundamentais, que acompanhe o progresso da sociedade e os seus novos desafios e exigências, sem deixar, todavia, que tal interpretação se transforme em algo que possa afetar e colidir, de um modo injustificado e ilimitado, com o núcleo essencial de cada um dos direitos.

As restrições são, constitucionalmente, autorizadas, por via do artigo 18.º da CRP, devendo, contudo, observar o princípio da proteção do núcleo essencial, compatibilizando-o com os princípios da dignidade da pessoa humana e da proporcionalidade (adequação aos fins do direito, indispensabilidade da restrição quando comparada com outras medidas que possam ser aplicadas, racionalidade e ponderação entre prejuízos e benefícios da sua aplicação e generalidade e abstração, no sentido de não poder identificar pessoas e casos na sua previsão legal).

"Como hoje soa consensual e pacífico entre os autores e os tribunais, e sobretudo do lado da jurisprudência constitucional, os direitos fundamentais são, em si e de per si, dinâmicos e abertos ao futuro, não dependendo a sua revelação e expansão de prévia e necessária intervenção do legislador. Diferentemente, a sua limitação e compressão, em nome dos fins e dos interesses do processo penal, estão sempre dependentes da acção insuprível do legislador"[92].

A apreensão do correio eletrónico, enquanto meio de obtenção de prova, afeta bens jurídicos pessoais que atingem a esfera privada, normalmente, de mais de uma pessoa, quer a do autor, quer a do(s) destinatário(s) da mensagem. Esta facto origina, por vezes, alguns problemas de identificação do titular[93] do bem jurídico, isto é, das pessoas que, concretamente, possam ser afetadas com a revelação das mensagens.

Por esta razão, o acesso ao correio eletrónico é regulado, de forma expressa e clara, evitando a interferência abusiva e a afetação do núcleo essencial dos direitos fundamentais em causa.

[92] COSTA ANDRADE – "*Bruscamente*, p. 150.
[93] Consideramos que o titular do bem jurídico tanto pode ser o autor da correspondência como o destinatário, enquanto destinatário e parte integrante daquele ato comunicacional. No mesmo sentido TRL – Acórdão de 24 de setembro de 2013, processo n.º 145/10.9GEALM.L2-5.

"Trata-se de uma preocupação de natureza material, que pretende evitar o esvaziamento dos direitos restringidos, nem tudo se permitindo, em nome do valor, direito ou interesse que pseudo-fundamentasse a restrição em questão"[94].

A estrutura normativa do CPP deve estar em sintonia com as normas e princípios da CRP, predominando uma ideia de concordância prática dos DLG, constitucionalmente, consagrados, com a trilogia de objetivos do processo penal, a descoberta da verdade material a par da justiça, a defesa dos direitos de todos os intervenientes no processo e a manutenção da segurança jurídica.

"A realização da justiça do caso é um valor constitucional, mas não é um valor absoluto, que possa ser perseguido por qualquer forma. Quando os meios utilizados para a obtenção de prova forem proibitivos ou condicionados pela Constituição para salvaguarda de outros valores, os elementos probatórios por essa razão obtidos não podem ser utilizados em circunstância alguma; ficam radicalmente inquinados do vício da inconstitucionalidade e o sistema não pode tolerar que a justiça seja prosseguida por meios inconstitucionais"[95].

Também no plano internacional se verifica a preocupação com a garantia e proteção destes direitos. No artigo 12.º da DUDH estabelece-se que ninguém pode estar sujeito a interferência na sua vida privada. No artigo 8.º, n.º 1 da Convenção Europeia dos Direitos do Homem (CEDH) consagra-se o direito ao respeito da correspondência, permitindo o acesso à mesma apenas nos termos previstos na lei.

Existe uma efetiva proteção do sigilo da correspondência e das comunicações e só em casos excecionais é permitida uma restrição deste direito.

Estamos perante a chamada colisão imprópria de direitos fundamentais, onde os direitos à defesa, à segurança e à administração da justiça têm de fazer cedências, em prol uns dos outros, para garantir uma certa harmonização e efetividade do sistema jurídico.

"Pensando nos interesses em jogo, a restrição de DLG funda-se na circunstância de os textos constitucionais reconhecerem que não seria possível a vida coletiva se não fossem previstos mecanismos de limitação material dos direitos fundamentais genericamente

[94] BACELAR GOUVEIA – *Manual*, p. 1009.
[95] MIRANDA, Jorge; MEDEIROS, Rui – *Constituição Portuguesa Anotada. Tomo I*. Coimbra: Coimbra Editora, 2005. p. 362.

proclamados, com o intuito primordial de assegurar a própria efetividade da respetiva tipologia no seu conjunto"[96].

"Os direitos fundamentais não são direitos infalíveis e, por isso, existem perigos que atualmente se concebem e que podem lançar dúvidas quanto à efetividade da sua proteção"[97].

Desta forma, e ainda que a CRP contemple de forma clara a proteção do sigilo e da ingerência nas comunicações, não raras vezes, somos confrontados com alguma incapacidade quanto ao acompanhamento da evolução tecnológica. O *modus operandi* dos potenciais agentes acaba por trazer alguns perigos não só para a vida na sociedade, mas também para a própria investigação e, em consequência, para a boa administração da justiça.

"Simplesmente, esses perigos, em vez de nos fazerem esmorecer, devem suscitar a nossa reflexão, tendo em mente o desiderato de os vencer. O Estado de Direito assim o exige"[98].

[96] BACELAR GOUVEIA – *Manual*, p. 1005.
[97] *Idem*, p. 942.
[98] *Ibidem*.

3. A não equiparação do correio eletrónico à correspondência tradicional

Ainda antes de entrarmos na questão da não equiparação do correio eletrónico relativamente à correspondência tradicional importa atentar alguns conceitos.

Por correspondência deve entender-se toda a troca, por norma, privada[99] de informação entre duas pessoas.

"A comunicação, diferentemente da informação, pressupõe uma relação de intersubjetividade, na qual o propósito é transmitir uma mensagem"[100].

Se antes a correspondência por excelência era a carta, com a evolução dos tempos, a carta tem dado lugar ao correio eletrónico cujo processo se realiza de um modo diferente.

Isto significa que não está em causa a consideração do correio eletrónico como uma forma de comunicação, mas apenas a discordância com a sua equiparação legal à correspondência tradicional.

Várias são as posições da doutrina quanto a esta questão que contribuem, por um lado, para o esclarecimento do nosso pensamento, mas por outro, para alguma confusão, o que acaba por se refletir tanto na interpretação como na aplicação da lei pelos tribunais.

3.1. As várias posições da doutrina

Tem-se defendido que o correio eletrónico a partir do momento em que é recebido e alocado num sistema informático, independentemente de ter sido aberto ou não, terá o valor probatório equivalente ao de um mero documento e, por essa razão, o meio de obtenção de prova que deverá ser utilizado é a apreensão de documento, previsto nos artigos 164.º e seguintes do CPP. [101]

Com base nesta corrente, verifica-se que, de certa maneira, o artigo 17.º da LC não teria qualquer aplicação na realidade, uma vez que quando o correio está em curso aplica-

[99] Embora possamos ter também correspondência pública como é o caso da carta aberta, todavia, este tipo de comunicação não estará abrangido pela tutela da correspondência.
[100] NEVES – *As ingerências*, p. 15.
[101] Cfr. BRAVO, Rogério – "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta". *Polícia e Justiça*. Coimbra: Coimbra Editora, 2006. N.º 7 (jan.jun. 2006) III Série, p. 209 e VERDELHO – *RMP*. Ano 25. N.º 100 (outubro/dezembro 2004), p. 158 e 159.

se o artigo 18.º da LC e assim que é rececionado pelo destinatário aplica-se o regime da apreensão de documentos.

Ainda dentro desta corrente, existe alguma divergência quanto à natureza do correio eletrónico. Se uns consideram que a equiparação à carta tradicional fica, completamente, enviesada porque o correio eletrónico tem uma natureza imaterial e, por isso, a sua eliminação não tem as mesmas consequências que a eliminação de uma carta[102], outros defendem que a mensagem de correio eletrónico pode ser arquivada e eliminada tal como a carta tradicional[103].

Sob outra perspetiva, tem-se rejeitado a equiparação em qualquer momento, ou seja, quer quando ainda é comunicação, quer quando já se considera ficheiro em formato digital. Sendo que o momento em que se considera que a comunicação termina é posterior ao defendido pela corrente anterior. Neste caso, o fator determinante não será a receção da mensagem, mas sim o "pleno domínio do destinatário, sendo por este conhecida"[104].

Esta corrente nega a inclusão do correio eletrónico, enquanto meio de comunicação eletrónico, no n.º 1 do artigo 179.º do CPP, onde se refere "qualquer outra correspondência".

Alerta-se, ainda, para a criação de vários obstáculos à investigação se aplicarmos o regime do artigo 179.º do CPP, como o facto de se exigir que o juiz seja o primeiro a tomar conhecimento do conteúdo da correspondência apreendida. Pensemos, por exemplo, numa investigação em que existem centenas de mensagens de correio eletrónico que têm de ser conhecidas e selecionadas por uma única pessoa e nas consequências negativas que tal exigência poderá trazer para a investigação.

Inclusivamente, podem surgir impossibilidades fácticas resultantes da natureza do correio eletrónico. Quando o juiz considera que as mensagens não têm relevância para o processo, a devolução que é exigida pelo n.º 3 do artigo 179.º não é possível quando estão em causa mensagens de correio eletrónico, uma vez que o acesso à conta é vedado e "não

[102] BRAVO – *Polícia*, 2006. N.º 7 (jan.jun. 2006) III Série, p. 212 e 214.
[103] VERDELHO – *RMP*. Ano 25. N.º 100 (outubro/dezembro 2004), p. 157 e 158.
[104] NEVES – *As ingerências*, p. 187.

se pode restituir correspondência virtual que foi gravada para ser levada ao juiz, mas que, no fundo, nunca saiu do computador/espaço virtual onde se encontrava"[105].

No caso de o visado ser o remetente da mensagem, ainda que se apreendam as mensagens por ele enviadas, não se poderá impedir que o respetivo destinatário tenha acesso às mesmas e que possa afetar a comunicação e, em consequência, inviabilizar a investigação.

Existem, ainda elementos, que não fazem parte do conteúdo da correspondência tradicional, mas que se revelam essenciais para a boa prossecução da investigação e para a descoberta dos factos como a identificação do equipamento de telecomunicação, a sua localização, a data, a hora, os chamados dados de base e de tráfego.

Enquanto na correspondência a ingerência de terceiros termina com a colocação da carta na caixa de correio, no caso do correio eletrónico, mesmo que a mensagem já tenha sido recebida e até lida pelo destinatário, esta continua acessível ao operador de comunicações eletrónicas.

3.2. Posição adotada

Se atentarmos na definição de correio eletrónico presente na Diretiva n.º 2002/58/CE, não encontramos qualquer referência ao conceito de correspondência, o que poderá demonstrar que não deve estabelecer-se qualquer equiparação ou aproximação à correspondência tradicional.

O correio eletrónico, quer do ponto de vista técnico, pelas suas características e pela forma como se processa, quer do ponto de vista jurídico, pelas exigências e especificidades na sua obtenção, embora seja também uma forma de comunicação que é protegida pela CRP, tal como a correspondência tradicional, não é, de todo, idêntico a esta.

A mensagem e o seu conteúdo merecem a proteção constitucional atribuída à correspondência e a outros meios de comunicação. Ainda assim, a danosidade causada

[105] NEVES – *As ingerências*, p. 185.

pelo acesso ao correio eletrónico é, completamente, diferente daquela que se gera quando acedemos a uma carta tradicional.

Quanto à sua natureza, a correspondência tradicional caracteriza-se por ser "um objeto, corporizado e fechado quando remetido e no caso, para efeitos desta discussão, estar fechada quando o executor da diligência a encontra, seja no decurso de uma busca, ou mesmo de uma revista"[106]. Em contrapartida, o correio eletrónico "nunca é, nem nunca está "fechado""[107] e "nem é o facto de uma mensagem electrónica deixar de estar em trânsito e de se fixar num sistema informático e poder por isso ser guardada ou destruída, que a caracteriza como correio em sentido tradicional: a sua natureza imaterial também a torna diferente da primeira"[108].

A doutrina maioritária parece apontar no sentido de o correio eletrónico "dever ser tratado em Direito Processual Penal como correspondência tradicional e dever, por isso, merecer os mesmos efeitos legais, mormente o de ter de ser o JIC a primeiro a tomar conhecimento do conteúdo do correio electrónico que se encontre num sistema informático"[109].

O que está em causa é a garantia da proteção dada pela CRP ao sigilo da correspondência e de outros meios de comunicação, onde consideramos dever integrar-se o correio eletrónico.

Mas não só, está também em causa o direito à reserva da intimidade da vida privada, uma vez que, como já referimos, anteriormente, há uma maior e mais lesiva intromissão quando se acede ao correio eletrónico do que quando se acede a uma carta isolada.

Pretende-se proteger a própria comunicação e o conteúdo dela resultante, assim como os direitos fundamentais das pessoas nela envolvidas.

Em suma, o correio eletrónico é um meio de comunicação eletrónico que merece a proteção constitucional atribuída pelo artigo 34.º da CRP. Todavia, isso não significa que

[106] BRAVO – *Polícia*, 2006. N.º 7 (jan.jun. 2006) III Série, p. 212.
[107] *Ibidem*.
[108] *Ibidem.*
[109] *Idem*, p. 207 e 208.

do ponto de vista legal, a sua conceção deva corresponder a uma equiparação, *tout court*, à correspondência tradicional.

O facto de existir uma remissão legal para o regime da correspondência na sua obtenção, como iremos abordar *infra*, também não significa que se deva equiparar, sem mais, o correio eletrónico à correspondência.

3.3. Conclusões

Não obstante parte da doutrina rejeitar a equiparação, tal não significa que não estejamos no domínio da correspondência ou das comunicações que merecem a tutela constitucional, pela ingerência na privacidade e nas comunicações.

E ainda que a tutela constitucional seja a mesma, a que se encontra no artigo 34.º da CRP, a sua concretização traz exigências diferentes consoante a forma de correspondência ou comunicação que está em causa.

Na definição de correio eletrónico presente na alínea h) do artigo 2.º da Diretiva n.º 2002/58/CE de 12 de julho de 2012 não há qualquer referência ao conceito de correspondência tradicional o que demonstra que não deve existir qualquer equiparação.

Na verdade, consideramos que o facto de existir uma definição do conceito de correio eletrónico, mostra que este deve ser autonomizado relativamente à correspondência tradicional.

A própria forma como a comunicação se processa, as características que apresenta, pela forma como é realizada mostra que, embora sejam formas de comunicação, a correspondência tradicional e o correio eletrónico não são idênticos e o acesso aos mesmos procede-se de formas, totalmente, distintas.

Importa ter em consideração, principalmente, a natureza das formas de comunicação em causa que, neste caso, justificam o tratamento diferenciado do ponto de vista legal.

A correspondência tradicional respeita a uma realidade material, palpável, que está efetivamente fechada quando ainda está em curso.

Por outro lado, o correio eletrónico corresponde a uma realidade digital e imaterial e, por essa razão, não se encontra efetivamente fechada ou aberta, mesmo quando ainda está

em trânsito, inclusive porque o seu processo de transmissão está dependente da autorização do servidor do programa de correio eletrónico utilizado que tem acesso à informação que é transmitida, nomeadamente para decidir quanto à permissão de transmissão.

Tendo em consideração a materialidade da primeira e a imaterialidade da segunda a sua destruição tem consequências práticas bastante diferentes

"A doutrina maioritária aposta no sentido de o correio-electrónico dever ser tratado em Direito Processual Penal como correspondência tradicional e dever por isso merecer os mesmos efeitos legais, mormente o de ter de ser o JIC o primeiro a tomar conhecimento do conteúdo do correio electrónico que se encontre num sistema informático"[110].

Acolhemos a posição de quem afirma que várias foram as oportunidades nas reformas, quer da lei substantiva, quer da lei processual para proceder a uma equiparação legal de ambas as formas de comunicação, mas tal não aconteceu e isso demonstra que não deve existir uma verdadeira equiparação.[111]

Aliás, o facto de não se ter incluído o correio eletrónico no artigo 179.º do CPP e ter-se criado um artigo autónomo demonstra que, ainda que possa existir uma remissão legal no regime estabelecido, não deve existir uma equiparação entre os dois meios de comunicação.

A realidade adjacente à criação do regime previsto no artigo 179.º do CPP revela-se bastante diferente da realidade em que se insere o correio eletrónico.

"A apreensão de um e de outro não afectam exactamente os mesmos direitos fundamentais e existem diferenças substanciais entre o correio corpóreo e as mensagens de correio electrónico e, consequentemente, com o campo de aplicação do artigo 179.º e do artigo 17.º da LC"[112].

[110] BRAVO – *Polícia*, 2006. N.º 7 (jan.jun. 2006) III Série, p. 207 e 208.
[111] *Idem*, p. 210.
[112] CARDOSO – *RMP*. Ano 39. N.º 153 (jan -mar 2018), p. 199.

4. A distinção jurisprudencial entre correio aberto e fechado

4.1. A mensagem aberta e a mensagem fechada

Na "nova" realidade onde se integra o correio eletrónico, o tratamento dado às mensagens abertas e lidas, aparece como um dos pontos que mais carece de esclarecimento quanto à sua tutela constitucional e processual penal, gerando controvérsia e exigindo um inevitável debate.

A problemática existente em torno da diferenciação entre a mensagem de correio eletrónico aberta e fechada não surgiu apenas com a LC. A reforma do CPP de 2007, onde se introduziu no seu artigo 189.º a referência às comunicações "mesmo que se encontrem guardadas em suporte digital", gerou alguma controvérsia. Sendo que, quer na doutrina, quer na jurisprudência, muitos foram os que ignoraram este novo elemento e as consequências que daí se deveriam retirar[113].

No artigo 17.º da LC manteve-se a referência a "armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro", pelo que toda a discussão, quanto a esta matéria continuou. Ainda que se tenha optado por manter a referência, não se aproveitou a oportunidade para criar um regime claro e inequívoco que esclarecesse, de forma expressa e detalhada, qual deveria ser o tratamento dado às mensagens abertas e fechadas. Em consequência, continua a existir divergência na doutrina e na jurisprudência.

A letra da lei, referindo-se aos dados armazenados, não estabelece qualquer distinção entre correio eletrónico aberto e fechado. Por esta razão, e numa interpretação literal, tanto ao primeiro como ao segundo deve ser aplicado o regime previsto no artigo 17.º da LC[114] que remete para o regime da apreensão de correspondência do CPP.

Deste modo, de acordo com o, expressamente, previsto no artigo 17.º da LC, independentemente de a mensagem estar aberta ou fechada, a sua apreensão carece sempre da intervenção por parte do juiz competente, ordenando ou autorizando a

[113] A não distinção entre a mensagem aberta e fechada ou, por outras palavras, a atribuição da proteção, dada às comunicações, ao conteúdo resultante das mesmas ainda que o processo comunicacional, em si, já tenha cessado.
[114] No mesmo sentido, RAMALHO, David Silva – *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017, p. 278 e 279.

diligência, o que permite concluir que deve existir uma maior proteção e tutela da mensagem de correio eletrónico do que a atribuída aos documentos.

"Não é juridicamente correto, nem tecnicamente adequado, interpretar o artigo 17.º de forma diferente para mensagens abertas e mensagens não abertas"[115].

Significa, portanto, que se quis atribuir "um *plus* de proteção a arquivos que já foram comunicação, em nome da salvaguarda da privacidade e da autodeterminação informacional"[116].

Por outro lado, se adotarmos uma interpretação que tenha em consideração as eventuais diferenças entre as mensagens abertas e fechadas[117] e a necessidade de uma tutela diferente em cada caso poderá ignorar-se o elemento literal e excluir do âmbito da norma a mensagem aberta, considerando-a como mero documento[118]. Desta forma, a sua apreensão não dependerá do cumprimento de certos requisitos formais, bastando apenas despacho da autoridade judiciária competente, de acordo com o n.º 1 do artigo 16.º da LC[119].

Nesta linha, argumenta a doutrina que o que já não é comunicação não pode merecer a tutela, nem estar sujeito ao regime aplicável ao que ainda é considerado como comunicação.[120]

Em suma, parte da doutrina, ainda que com argumentação diversa, defende um tratamento diferenciado entre as mensagens abertas e lidas e as mensagens fechadas, afirmando que após a abertura da mensagem, a comunicação já terminou, pelo que se trata apenas de um mero documento, em suporte digital, não beneficiando da proteção

[115] CARDOSO – *RMP*. Ano 39. N.º 153 (jan -mar 2018), p. 186.
[116] NEVES – *As ingerências*, p. 177.
[117] *V.g.* o facto de as mensagens abertas já se encontrarem na esfera de domínio doo destinatário.
[118] Tendo, por isso, a mesma proteção que as cartas recebidas, abertas e guardadas nos termos dos artigos 178.º e 179.º do CPP.
[119] Ainda que no casso do n.º 3 do artigo 16.º da LC se preveja que no caso de "dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto".
[120] Neste sentido, CONDE CORREIA – *RMP*. Ano 35. N.º 139 (julho-setembro 2014), p. 41 e MESQUITA, Paulo Dá – *Processo Penal, Prova e Sistema Judiciário.* Coimbra: Wolters Kluver Portugal, 2010. p. 118.

dada à correspondência e às comunicações, podendo, por isso, ser livremente apreendida.[121]

Quanto ao momento em que a mensagem deixa de ser comunicação, a maioria da doutrina acolhe o entendimento segundo o qual após a sua abertura esta deixa de merecer a tutela das comunicações, passando apenas a gozar da tutela conferida aos documentos.

No entanto, quando a mensagem já foi recebida, mas ainda não foi lida, somos confrontados com duas aceções. Por um lado, há quem considere que a mensagem ainda não está no total domínio do destinatário e como tal ainda pode ser intercetada enquanto comunicação[122]. Por outro, há quem defenda a aplicação do regime da interceção quando a mensagem está a ser transmitida, o regime da apreensão de correspondência quando a mensagem já foi recebida, mas ainda não foi lida pelo destinatário e o regime da apreensão de documentos quando a mensagem já foi aberta e lida pelo destinatário[123].

"Obviamente que a mensagem não perde o seu interesse para a investigação criminal por não ser comunicação em trânsito. Aliás, mantém o teor da mensagem o mesmo interesse investigatório que tinha antes de iniciar o seu percurso comunicacional. O que se altera é o seu estatuto, o que muda é o seu estado"[124].

Podem surgir dúvidas quanto à aferição da abertura ou não da mensagem, uma vez que existem programas que permitem assinalar como não lidas as mensagens que tenham sido abertas.[125] Nestes casos, tem-se defendido[126] que a apreensão deve ser realizada como se se tratasse de mensagens de correio eletrónico fechadas.

4.2. A Jurisprudência

Se na doutrina não há consenso, tal irá refletir-se, em grande medida, na jurisprudência, onde a divergência e a contradição nas decisões gera uma instabilidade

[121] Cfr. CONDE CORREIA – *RMP*. Ano 35. N.º 139 (julho-setembro 2014), p. 140; VERDELHO – *RMP*. Ano 25. N.º 100 (outubro/dezembro 2004), p. 157 e 158 e NEVES – *As ingerências*, p. 182 e COSTA ANDRADE – *"Bruscamente*, p. 159.
[122] ANDRADE – "*Bruscamente*, p. 159.
[123] VERDELHO – *RMP*. Ano 25. N.º 100 (outubro/dezembro 2004), p. 157.
[124] NEVES – *As ingerências*, p. 183.
[125] Quanto a esta questão, da mesma forma que existem programas que permitem alterar o estado da mensagem, também existem programas que permitem verificar se a mensagem já foi, efetivamente, aberta ou não. Por outro lado, o facto de a mensagem não estar aberta não significa que a mesma não tenha sido lida, uma vez que é possível, por exemplo, através de programas como o *WebMail*, pré-visualizar a mensagem, incluindo todo o conteúdo, sem que esta seja aberta.
[126] Cfr. VERDELHO – *RMP*. Ano 25. N.º 100 (outubro/dezembro 2004), p. 159.

indesejada que ameaça princípios como os da boa administração da justiça e da sua tutela efetiva, direitos fundamentais e as próprias garantias do processo penal.

A jurisprudência que apresentaremos no presente ponto respeita à apreensão de mensagens de correio eletrónico e à apreensão de *SMS*. Consideramos que se deve aplicar, a ambas, o regime previsto no artigo 17.º da LC por se tratar de dados armazenados em suporte digital, resultantes do envio de mensagens de correio eletrónico ou de comunicações de natureza semelhante, pelo que o enquadramento legal das *SMS* deve ser o mesmo que o das mensagens de correio eletrónico.[127]

4.2.1. A mensagem aberta como mero documento

Em desconsideração da expressão "guardadas em suporte digital", quer quando se aplicava o artigo 189.º do CPP, até 2009, quer, posteriormente e até aos dias de hoje, com a aplicação do artigo 17.º da LC[128], parte da jurisprudência tem optado por estabelecer uma distinção entre a mensagem aberta e a mensagem fechada. Depois de aberta e lida corresponde a um mero documento, deixando, portanto, de pertencer à área das comunicações e gozando apenas da proteção que os documentos merecem.

Relativamente à mensagem aberta, como o ato comunicacional, em sentido estrito, já cessou e esta já se encontra na esfera de domínio do destinatário corresponde a um mero documento. Deixa, portanto, de pertencer à área das comunicações, gozando apenas da proteção que todos os documentos merecem, aplicando-se o regime previsto no artigo 178.º do CPP[129].

Cumpre, contudo, referir quanto a esta questão que ao considerar-se a mensagem aberta como um mero documento ao qual é aplicável o regime do artigo 178.º do CPP, a jurisprudência está a ignorar o facto de a mensagem de correio eletrónico corresponder a dados informáticos, nomeadamente dados de conteúdo, com uma proteção acrescida.

---

[127] Neste sentido, GABINETE CIBERCRIME – "Nota Prática n.º 6/2015 de 27 de agosto de 2015". Procuradoria Geral da República - *Jurisprudência sobre prova digital*. p. 2.
Como veremos *infra*, no ponto referente ao regime da apreensão de correio eletrónico, por coerência de pensamento, consideramos que a apreensão de mensagens de correio eletrónico através de um telemóvel deve submeter-se ao regime do artigo 17.º da LC, uma vez que o que está em causa é o sistema informático e os dados que estão nele armazenados.
[128] Que refere "armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro".
[129] Não carecendo de autorização judicial pode ser, desse modo livremente apreendida.

Por essa razão, ainda que se estabeleça a distinção entre mensagens abertas e fechadas, e, em consequência, não se atribua a proteção constitucional das comunicações às mensagens abertas, não deveria ser aplicado o regime do artigo 178.º do CPP mas sim o regime previsto no artigo 16.º da LC respeitante à apreensão de dados informáticos.

Quanto à mensagem fechada, embora o ato comunicacional, em sentido estrito, já tenha cessado, como a mensagem ainda não se encontra na esfera de domínio do destinatário, por não ser por ele conhecida, deve continuar abrangida pela tutela das comunicações. Deve, por isso, aplicar-se o regime previsto no artigo 17.º da LC que remete para o regime da apreensão de correspondência do CPP[130].

Neste caso, para quem considera que deve existir uma distinção entre a mensagem aberta e a mensagem fechada, o grande argumento é o de que o conteúdo resultante da comunicação, que se encontre armazenado, já não pertence à área das telecomunicações, pelo que apenas a correspondência fechada, sigilosa por natureza, goza, da proteção constitucional do artigo 34.º, n.º 1 da CRP.[131]

O TRL, com o qual o TRP[132] concorda, vai mais longe numa das suas decisões[133], e ainda que anterior à LC, para além de estabelecer a distinção entre a mensagem aberta e fechada, presume que "a mensagem uma vez recebida, foi lida pelo seu destinatário"[134].

Concluímos que um dos pontos comuns em quase todas as decisões aqui referidas é o da invocação de jurisprudência anterior a 2007 como orientação para decidir de determinada forma.

Ora, antes de 2007 ainda não existia a expressa menção às mensagens "guardadas em suporte digital"[135] ou "armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro"[136], pelo que nos parece que nem as

[130] Artigo 179.º do CPP.
[131] Neste sentido TRL – Acórdãos de 2 de março de 2011 e de 24 de setembro de 2013 processos n.º 463/07.3TAALM-A.L1-3 e 145/10.9GEALM.L2-5 respetivamente.
[132] TRP Acórdão de 27 de janeiro de 2010, processo n.º 896/07.5JAPRT.P1, que defende que "A mensagem via telemóvel já recebida deverá ter o mesmo tratamento da correspondência escrita, que circula através do tradicional sistema postal: recebida mas ainda não aberta pelo destinatário, aplicar-se-á, à respectiva apreensão, o estabelecido no artigo 179º do CPP; recebida, aberta e guardada pelo destinatário, já não beneficiará do regime de protecção da reserva da correspondência e das comunicações, podendo ser apreendida para valer como mero documento escrito.".
[133] TRL – Acórdão de 15 de julho de 2008, processo. nº 3453/2008-5.
[134] TRL – Acórdão de 15 de julho de 2008, processo. nº 3453/2008-5.
[135] Artigo 189.º do CPP.
[136] Artigo 17.º da LC.

decisões aqui referidas, nem as que nelas são invocadas se mostram adequadas face ao regime atual.

Atualmente, a distinção entre mensagens abertas e fechadas não vai ao encontro da letra da lei e daquilo que resulta da alteração legislativa de 2007 ao artigo 189.º do CPP e, posteriormente, em 2009, com a LC, nem garante a proteção dos direitos fundamentais que estão aqui em causa.

Esta posição de diferenciação não é acolhida por toda a jurisprudência, existindo, por isso, decisões no sentido de que não deve existir qualquer distinção entre mensagens abertas e fechadas.

4.2.2. A mensagem aberta como merecedora da proteção das comunicações

Encontramos decisões que afirmam que não deve estabelecer-se qualquer distinção quanto ao regime aplicável às mensagens abertas e fechadas, não existindo, por isso, uma diminuição das exigências garantística entre as duas[137].[138]

Tal posição funda-se, principalmente, na letra da lei. Parece-nos que a expressão "armazenados nesse sistema informático…" não deixa margem para dúvidas, "a lei não estabelece qualquer distinção entre mensagens por abrir ou já abertas"[139].

Nem o artigo 189.º do CPP, até 2009, estabelecia, nem a CRP, nem o artigo 17.º da LC, atualmente, estabelecem qualquer distinção quanto às mensagens abertas e fechadas.[140]

Consideramos, por isso, que existe uma extensão do âmbito de tutela do regime aplicável às comunicações, às situações em que a comunicação, em sentido estrito, já

[137] Neste sentido, TRL – Acórdão de 20 de dezembro de 2011, processo n.º 36/11.6PJOER-A.L1-5.
[138] Posição com a qual concordamos.
[139] TRG – Acórdão de 29 de março de 2011, processo n.º 735/10.0GAPTL – A.G1.
[140] *Vide* TRL – Acórdão de 20 de dezembro de 2011, processo n.º 36/11.6PJOER-A.L1-5: "Nem a norma constitucional do art. 34.º n.º 1 da CRP nem as normas processuais penais fazem qualquer distinção entre correspondência fechada e correspondência aberta. Tal distinção não tem qualquer suporte na letra da lei. Não há uma diminuição de exigências garantísticas entre correspondência fechada e correspondência aberta. Independentemente de a correspondência ter sido ou não aberta ou de ter sido ou não lida, a pessoa a quem é dirigida tem sempre o direito de não ver essa correspondência devassada por terceiros. Constituindo a leitura da correspondência um atentado ao direito da inviolabilidade da mesma, só o juiz de instrução criminal pode, verificando-se os requisitos legais, determinar a apreensão de correspondência, validar a apreensão de correspondência, ser a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, e, ser quem decide se a mesma é ou não relevante.".

cessou, ou seja, ao resultado dessa comunicação, aos dados que se encontram armazenados no sistema informático. A extinção do ato comunicacional não corresponde ao fim do âmbito da tutela extensiva.[141]

Encontramos, ainda, decisões que, embora defendam que a lei continua a proteger a mensagem guardada[142], acabam por estender o regime da interceção ao momento em que o destinatário toma conhecimento do conteúdo da mensagem, uma vez que a comunicação ainda não está completa, o que significa que, nesta perspetiva, à mensagem recebida e não aberta aplicar-se-á o regime da interseção de comunicações.[143]

Não cremos, contudo, que tal possa fazer sentido. Consideramos que o elemento distintivo deve basear-se na natureza atualista em tempo real da intervenção.[144]

A LC, quanto às comunicações, prevê dois regimes processuais em que apenas se deve distinguir entre a interseção de comunicações, neste caso, de mensagens de correio eletrónico em tempo real aplicando-se o artigo 18.º da LC e a apreensão dessas mesmas mensagens quando se encontram armazenadas em sistema informático, aplicando-se o artigo 17.º da LC.[145]

Considera-se, portanto, que não se estabelece qualquer distinção entre a mensagem aberta e fechada e, por essa razão, aplica-se o regime do artigo 17.º da LC[146], que requer a intervenção do juiz para proceder à apreensão. No caso de não existir despacho do juiz e não tendo o titular do bem jurídico dado o seu consentimento, "estamos perante uma prova proibida de ser usada no processo"[147], "em nada relevando que os mesmos tivessem

[141] Neste sentido, DÁ MESQUITA – *Processo Penal,* p. 91 e TRG – Acórdão de 29 de março de 2011, processo n.º 735/10.0GAPTL – A.G1.
[142] Guardada leia-se aberta, lida e armazenada.
[143] Neste sentido TRG – Acórdão de 15 de outubro de 2012, processo n.º 68/10.1GCBRG.G1 que refere que "Entre o momento em que uma sms é enviada e aquele em que é lida medeia sempre algum tempo. Enquanto a mensagem não for "aberta" e lida pelo destinatário, a transmissão da comunicação não está completa. Durante todo esse tempo a sua interceção está sujeita às regras das interceções das comunicações telefónicas".
[144] Cfr. TRE – Acórdão de 6 de janeiro de 2015, processo n.º 6793/11.2TDLSB-A.E1.
[145] Neste sentido, TRL – Acórdão de 6 de fevereiro de 2018, processo n.º 1950/17.0 T9LSB-A.L1-5.
[146] Quanto à apreensão de mensagens fechadas e abertas, desde que se encontrem armazenadas em sistema informático.
[147] TRP – Acórdão de 12 de setembro de 2012, processo n.º 787/11.5PWPRT.P1.

sido ou não abertos e lidos pelo destinatário, pois que a lei não distingue entre essas duas situações[148]. Por conseguinte, estamos ante um caso de prova proibida"[149].

4.3. Conclusões

Há que distinguir entre o que é estalecido pela lei, ou seja, o regime que está em vigor e que deve ser respeitado e o entendimento que cada um pode ter relativamente a determinada matéria, não podendo, todavia, permitir-se que este último derrogue, sem mais, o primeiro.

Deve ter-se em consideração o que está previsto na norma e a aplicação da mesma, segundo o que nela se estabelece.

Podemos admitir o entendimento que cada um pode ter relativamente ao conceito de comunicação e à proteção que lhe deve ser atribuída, quando ainda está em trânsito e quando já cessou, e se se deve considerar que deve existir ou não um tratamento diferenciado.

Porém, tal não pode ter como consequência o desvirtuamento da norma e da proteção constitucional da mensagem.

As mensagens arquivadas num sistema informático gozam ainda da proteção dada às comunicações, pelo que a sua obtenção, leitura ou utilização por parte dos OPC deve ser precedida de autorização judicial.

Não se podem diminuir as garantias previstas, expressamente, na lei por via interpretativa.

"A prolação de Despacho judicial afigura-se assim claramente imprescindível"[150], ou seja, qualquer mensagem recebida, independentemente de estar aberta e lida ou fechada, só pode ser admitida no processo como prova se tiver existido uma autorização judicial, prévia à apreensão, nesse sentido.

[148] No mesmo sentido se pronuncia TRG – Acórdão de 29 de março de 2011, processo n.º 735/10.0GAPTL – A.G1.
[149] TRP – Acórdão de 12 de setembro de 2012, processo n.º 787/11.5PWPRT.P1.
[150] TRP – Acórdão de 22 de maio de 2013, processo n.º 74/07.3PASTS.P1.

O que está em causa é a exigência ou não de despacho judicial para se proceder à apreensão e leitura das mensagens.

A partir do momento em que se distingue a mensagem aberta da mensagem fechada e se defende a aplicação do regime do artigo 178.º do CPP, relativamente às mensagens abertas, elimina-se a exigência de despacho do juiz, sendo, portanto, as mesmas livremente apreensíveis, independentemente do consentimento do visado.

Ora, para quem procede às diligências e coordena a investigação, poderá ser mais profícuo, em termos de gestão do processo, não fazer depender a apreensão de uma autorização judicial prévia e o conhecimento das mesmas da leitura, em primeiro lugar, pelo juiz. Contudo, não podemos permitir que o reconhecimento dessa utilidade derrogue a letra da lei.

Até 2009, quando se aplicava o 189.º do CPP e já depois da Reforma de 2007 que acrescentou "guardadas em suporte digital", muitas foram as decisões[151] que adotaram uma interpretação *contra legem* deste preceito. Cremos que a inclusão deste trecho pretendeu reforçar a proteção das mensagens, independentemente do seu estado. Entendemos, por isso, que a apreensão e a subsequente junção ao processo dependem da intervenção do juiz por ainda estar abrangida pela norma e por não se tratar apenas de mero documento.

A LC manteve esta posição de proteção, uma vez que se refere também aos dados armazenados.

Consideramos que, com base no texto da lei e tendo em conta a proteção constitucional dos direitos que potencialmente possam ser afetados, não deve existir qualquer distinção entre as mensagens abertas e fechadas.

"Da leitura conjugada dos preceitos citados, nomeadamente do artº 179º nº 1 e 3 e 178 nº3 do CPP, não vemos incompatibilidade alguma mas sim complementaridade e não nos parece que haja sido intenção do legislador, atendendo aos princípios e escopo subjacentes, fazer qualquer distinção nos sobreditos preceitos entre "correspondência aberta ou fechada", mas apenas a

[151] Exemplo de uma dessas decisões, TRG – Acórdão de 12 de outubro de 2009, processo n.º 1396/08.1PBGMR-A.G1, ainda que se refira às SMS, sendo posterior à reforma do CPP de 2007 e à LC ignora a alteração, invocando inclusivamente jurisprudência anterior a 2007. Parece-nos, portanto, que a jurisprudência tem ignorado as alterações legislativas.

salvaguarda jurisdicional, com respeito de direitos fundamentais, v.g o da reserva da vida privada, de meios de prova através dos quais se acede ou há o perigo de aceder com alto grau de probabilidade a informações de natureza íntima ou com ela conexas. Daí que se exija que o juiz seja o primeiro a tomar conhecimento do conteúdo da correspondência (esteja ou não aberta e/ou lida), a analise, a julgue relevante ou não para a prova, faça juntar ao processo a que é relevante para a prova e, da que entenda não o ser, ordene seja devolvida a quem de direito.

A jurisprudência e doutrina que defendem a distinção entre a mensagem aberta e fechada "pautam-se por uma visão desgarrada dos bens e valores em protecção (a reserva e intimidade da vida privada), plasmados a partir do artº 34º nº1 da CRP descartando-se destes por via de argumentação centrada no facto de a correspondência estar ou não aberta, o que é completamente irrelevante, pois que o que se pretende é evitar sem controle judicial, em primeira mão, a devassa da vida privada ou de segredo profissional inerentes à correspondência apreendida através de acesso por terceiros ou mesmo por intervenientes processuais ao conteúdo daquela. Esse conteúdo deve ser sempre protegido e garantido, sempre que possível, por prévio controlo judicial"[152].

Podemos compreender os argumentos de quem defende que estamos perante situações distintas, pois quanto às mensagens abertas, o destinatário já tomou conhecimento e tem sobre as mesmas o poder de disponibilidade e quanto às mensagens fechadas tal não se verifica e que, por essa razão, a proteção deveria ser diferente. Todavia, quando nos confrontamos com o texto legal e com a proteção constitucional atribuída às mensagens de correio eletrónico enquanto comunicações, não podemos retirar tal conclusão, em virtude da menção expressa às mensagens armazenadas, não discriminando o seu estado.

Não consideramos correta nem prudente uma interpretação *contra legem* do preceito, que diferencie o regime aplicável com base nas diferentes conceções técnicas ou concetuais dos dois estados da mensagem.

"Cremos que se trata de uma distinção artificial, já que o que está em causa é evitar a devassa da dita correspondência por terceiros dada a natureza privada e íntima do seu conteúdo independentemente da forma como ela se apresente protegida"[153].

Na base do nosso pensamento encontra-se o princípio *Ubi lex non distinguit nec nos distinguere debemus*, que determina que onde a lei não distingue, não cabe ao intérprete

[152] TRL – Acórdão de 20 de dezembro de 2011, processo n.º 36/11.6PJOER-A.L1-5.
[153] TRL – Acórdão de 20 de dezembro de 2011, processo n.º 36/11.6PJOER-A.L1-5.

estabelecer qualquer distinção. Não existe qualquer referência quanto a uma possível distinção, pelo contrário, o tratamento deve ser o mesmo. Com a introdução do trecho "armazenados…" considera-se que deve atribuir-se a mesma proteção às mensagens, independentemente do seu estado pelo que não podemos tratar de uma forma diferenciada as mensagens abertas e fechadas.

Deve aplicar-se, sempre, o artigo 17.º da LC, independentemente de a mensagem estar aberta ou fechada. A apreensão de mensagens de correio eletrónico armazenadas em sistemas informáticos dependerá sempre da autorização ou ordem do juiz competente, bem como que seja este a tomar conhecimento, em primeiro lugar, do conteúdo das mesmas, para que estas possam ser admitidas no processo e valer como prova.

No fundo, o que se procura é o equilíbrio entre dois interesses conflituantes, por um lado, a eficácia da investigação e da ação penal e, por outro lado, a proteção de direitos fundamentais.

Não podemos, porém, na gestão do referido equilíbrio ignorar e derrogar a letra da lei, principalmente, quando tal conduz à existência de jurisprudência altamente contraditória e, por isso, violadora, entre outros, dos princípios da igualdade e do Estado de Direito democrático.

Capítulo III – A apreensão de correio eletrónico

1. O regime atual

1.1 O Código de Processo Penal até 2009

A apreensão do correio eletrónico, enquanto meio de obtenção de prova, foi introduzida no processo penal português com a revisão ao CPP de 1998. Procedeu-se a uma extensão do regime das escutas telefónicas às comunicações eletrónicas transmitidas por qualquer meio técnico diferente de telefone por via do artigo 190.º do mesmo diploma, correspondente ao atual artigo 189.º, passando, por isso, a ser um meio de obtenção de prova típico.

No atual artigo 189.º do CPP encontra-se, então, previsto o regime da apreensão de correio eletrónico, através de uma equiparação ao regime das escutas telefónicas presente nos artigos 187.º e 188.º também do CPP.

Com a reforma ao CPP de 2007 alargou-se o âmbito da extensão às comunicações guardadas em suporte digital. Manteve-se a proteção presente no regime das escutas telefónicas a qualquer forma de comunicação que implique a transmissão de dados por via telemática, acrescentando a inserção do conteúdo dessa transmissão guardado em suporte digital.

Em consequência, o regime das escutas passou a ser aplicado à interseção de comunicações, bem como à apreensão dos dados que delas resultam.

Ampliou-se o âmbito de tutela do regime das escutas telefónicas a situações em que o ato comunicacional, em sentido estrito[154], já cessou, incluindo-se o produto deste resultante, isto é, os dados informáticos recebidos e armazenados no suporte digital.

Neste sentido, entende-se que, independentemente de a mensagem se encontrar aberta ou fechada, para que esta possa ser apreendida, ser considerada no processo e ser utilizada como prova, tem de se respeitar o regime previsto nos artigos 187.º e 188.º do CPP, exigindo-se, nomeadamente a autorização do JIC para proceder à sua apreensão.[155]

[154] Enquanto dura a transmissão da informação.
[155] DÁ MESQUITA – *Processo Penal*, p. 91 e 92.

Para aqueles que afastavam a aplicação do regime das escutas telefónicas às comunicações já cessadas e armazenadas em suporte digital cremos que tal correspondia a uma interpretação excessivamente restritiva.

Foi este o regime que vigorou, entre nós, até 2009.

1.2. A Lei do Cibercrime de 2009

Como forma de acompanhar os "novos" tempos e a "nova" criminalidade, surgiu a Lei n.º 109/91, de 17 de agosto, conhecida como Lei da Criminalidade Informática, onde se definiu e previu os chamados crimes informáticos.

Ao longo do tempo, a sociedade e, em especial, a realidade informática evoluíram a uma velocidade inimaginável e com uma enorme complexidade, levando a uma clara desatualização da Lei da Criminalidade Informática.[156]

Internacionalmente, também houve produção legislativa, nomeadamente do Conselho da Europa, que influenciou a criação de uma nova lei.

A Lei n.º 109/2009, de 15 de setembro, entrou em vigor a 15 de outubro de 2009, a chamada Lei do Cibercrime que veio revogar, de forma expressa, a Lei da Criminalidade informática, transpondo para a ordem jurídica portuguesa a Decisão Quadro n.º 2005/222/JAI[157], do Conselho, de 24 de fevereiro e adaptando o direito interno à Convenção sobre o Cibercrime.

A criação da Convenção sobre o Cibercrime e da LC visou ampliar o âmbito de aplicação da Lei até onde existir a necessidade de obter prova com conteúdo que se encontre em qualquer sistema informático.

A LC é composta por três partes. A primeira relativa ao direito penal material onde se prevê os crimes informáticos, anteriormente previstos na Lei da Criminalidade Informática, atualmente revogada. A segunda relativa ao direito processual penal onde foram criados regimes de obtenção de prova e se adaptaram alguns já existentes ao mundo digital. A terceira relativa à cooperação internacional.

---

[156] Neste sentido VERDELHO, Pedro – "A nova Lei do Cibercrime". *Scientia Iuridica*, Braga: Universidade do Minho. T. LVIII. N.º 320 (out.- dez. 2009), p. 717 e 718.
[157] Relativa a ataques contra sistemas de informação.

Foquemo-nos na segunda parte da LC.

Quanto à parte processual pode afirmar-se que estão previstos dois regimes. Um regime geral presente nos artigos 11.º a 17.º da LC e um outro presente no artigo 18.º da LC que contém um catálogo e um regime especial.

O elemento distintivo entre os dois regimes funda-se no conceito de interceção em tempo real de comunicações. O artigo 17.º da LC refere-se a dados de tráfego e de conteúdo de correio eletrónico armazenados e o artigo 18.º da LC refere-se à interceção em termo real de dados de tráfego e de conteúdo.[158]

Esta distinção é importante, pois reforça o que foi defendido, anteriormente, quanto à não diferenciação entre mensagens abertas e fechadas, uma vez que se entende que apenas existe a distinção entre a interceção em tempo real e apreensão de dados armazenados.

O artigo 17.º da LC, respeitante à apreensão de mensagens de correio eletrónico, implicou uma alteração indireta ao CPP. O acesso ao correio eletrónico, implicando o acesso a um sistema informático, encontra-se, atualmente, regulado no artigo 17.º da LC, que remete para o regime da apreensão de correspondência do CPP.[159]

Neste caso, procurou-se "transpor para as novas formas de comunicar os mesmos princípios processuais da apreensão de correspondência, prevista no Código de Processo Penal"[160]. "Esta opção traduz uma ruptura com o sistema daquele Código, que opta por aplicar à apreensão de comunicações electrónicas (e não apenas à intercepção dessas comunicações), o regime da intercepção de comunicações telefónicas"[161].

[158] Neste sentido TRE – Acórdão de 6 de janeiro de 2015, processo n.º 6793/11.2TDLSB-A.E1 e TRE – Acórdão de 20 de janeiro de 2015, processo n.º 648/14.6GCFAR-A.E1.
[159] TRE – Acórdão de 20 de janeiro de 2015, processo n.º 648/14.6GCFAR-A.E1 – "Daqui resulta que o Código de Processo Penal deixa de ser aplicável aos dados informáticos armazenados ou interceptados nos seguintes trechos:
- ao correio electrónico ou outras formas de transmissão de dados por via telemática conservados (redacção dada pela Lei n.º 59/98, de 25 de Agosto);
- mesmo que se encontrem guardadas em suporte digital;
- aos dados, conservados, sobre a localização celular ou de registos da realização de conversações ou comunicações (redacção dada pela Lei n.º 48/2007, de 29/08).".
[160] VERDELHO – *Scientia*, T. LVIII. N.º 320 (out.- dez. 2009), p. 735.
[161] *Idem*, p. 743.

Até 2009, podemos afirmar que existia uma "equiparação" do correio eletrónico às comunicações telefónicas. Em 2009, uma lei especial, a LC, retirou-o do âmbito das escutas e integrou-o no âmbito da correspondência.

Admitimos que "a referida Lei do Cibercrime veio, de facto, alterar indelevelmente o direito probatório, na medida em que se propôs a estabelecer um conjunto de regras gerais (de processo penal) sobre meios de obtenção de prova no domínio dos *sistemas informáticos*"[162].

Tal trouxe consequências, por um lado, a nível concetual, pois o que antes era compreendido como comunicação eletrónica ou comunicação por meio diferente de telefone passou a ser entendido como correspondência. Por outro lado, implicou algumas alterações, a nível processual, uma vez que existiu um alargamento do seu âmbito de aplicação.

O regime das escutas telefónicas, por se tratar de um meio oculto de obtenção de prova, implica uma forte restrição ao direito fundamental da inviolabilidade das telecomunicações em tempo real. Por essa razão, é um regime muito mais restrito e exigente, nomeadamente quanto ao catálogo de crimes que permitem a sua utilização e quanto às fases em que a mesma é permitida, sendo restrita apenas à fase de inquérito.

Cumpre ainda referir que o regime das escutas telefónicas ao não permitir a utilização deste meio de obtenção de prova na investigação de crimes informáticos poderia inviabilizar o prosseguimento da investigação, por falta de acesso a prova indispensável e fundamental.

Atualmente, o catálogo de crimes encontra-se previsto no n.º 1 do artigo 11.º da LC, que permite a utilização deste método de obtenção de prova nos crimes previstos no mesmo diploma, cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

Significa, portanto, que a apreensão de correio eletrónico pode ser utilizada na generalidade dos crimes, desde que se verifique o interesse em proceder à recolha de prova em suporte eletrónico.

[162] TRG – Acórdão de 29 de março de 2011, processo n.º 1396/08.1PBGMR-A.G1 e DÁ MESQUITA – *Processo Penal*, p. 100.

No regime previsto pelo artigo 179.º do CPP, "a correspondência tem de ser expedida pelo suspeito/arguido ou lhe ser dirigida, mesmo que sob nome diverso ou através de pessoa diversa; na LCC, pode respeitar a qualquer pessoa (mais uma vez, o artigo 11.º não faz qualquer restrição de âmbito subjectivo)"[163].

Por outro lado, o regime é mais amplo, permitindo-se a sua utilização em qualquer fase do processo e não apenas durante a fase de inquérito, como acontece no regime das escutas telefónicas.

Todavia, é na fase de inquérito que surgem as grandes divergências, nomeadamente quanto às competências atribuídas ao Ministério Público (MP) e ao JIC.[164] Por essa razão, a abordagem a estas questões será feita no âmbito do inquérito.[165]

O regime da apreensão de correspondência, atualmente em vigor, encontra-se previsto no artigo 17.º da LC que remete para o regime da apreensão de correspondência do CPP.

As mensagens de correio eletrónico correspondem a dados informáticos, especificamente, dados de conteúdo, dados de base e dados de tráfego[166]. Deste modo, pode considerar-se que o regime estabelecido no artigo 17.º da LC é um regime especial de apreensão de dados informáticos face ao geral, previsto no artigo 16.º da LC. Contudo, por via da remissão presente no artigo 17.º da LC, consideramos que se aplica o regime da apreensão de correspondência, na parte em que não for contrária ao artigo 17.º e não o artigo 16.º, ambos da LC.

1.3. A remissão para o regime do artigo 179.º do CPP

Quando o CPP foi criado, em 1987, a prova digital não era uma realidade tal como hoje se apresenta e, portanto, não havia qualquer previsão legal quanto a esta matéria.

[163] CARDOSO – *RMP*. Ano 39. N.º 153 (jan -mar 2018), p. 191.
[164] *Idem*, p. 168.
[165] Na fase de inquérito, o *dominus* do processo é o MP, exigindo-se nas situações que serão abordadas *infra* despacho do JIC. Nas restantes fases do processo a questão não se coloca, uma vez que o *dominus* do processo é o JIC e, por essa razão, tanto no caso do artigo 16.º como nos do artigo 17.º, ambos da LC, tem de existir despacho do JIC.
[166] Nos cabeçalhos técnicos.

Com o aparecimento da prova digital, novas realidades foram sendo integradas no nosso ordenamento jurídico, quer através da incorporação de novos regimes, quer através da adaptação dos regimes já existentes aos que vão surgindo.

"As mensagens de correio electrónico ou registos 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"[167].

A remissão surgiu como uma forma de integrar esta nova realidade e permitir que as mensagens, enquanto meio de prova relevante, sejam admitidas no processo de forma legal, adaptando-se o regime e não através de uma aplicação integral e acrítica.[168]

Significa, portanto, a aplicação do regime da correspondência na medida em que este não contrarie o previsto na LC, ou seja, a remissão não pode sobrepor-se ao regime especial de apreensão previsto no artigo 17.º da LC.[169]

Em 2009, a LC refletiu uma nova opção político criminal. Alterou-se o regime aplicável, deixando de remeter-se para o regime das escutas telefónica, passando a remeter-se para o regime da apreensão de correspondência, o que reflete dois aspetos.

Por um lado, a consciência de que, do ponto de vista da investigação criminal, o correio eletrónico passou a ser um elemento fundamental para apurar a verdade dos factos e que deve ser passível de apreensão em qualquer fase do processo, de modo a permitir esse mesmo apuramento e a obtenção de mais e melhor prova.

Por outro lado, e, em parte, em consequência desta alteração, tem-se conseguido obter mais e melhores resultados nas investigações que envolvem o acesso a sistemas informáticos.

De certa forma, o regime das escutas telefónicas acabava por limitar a investigação criminal. Alterou-se o regime prevendo-se uma solução menos restritiva, que visa uma maior facilidade de acesso e, em consequência, a boa prossecução da investigação.

[167] TRL – Acórdão de 11 de janeiro de 2011, processo n.º 5412/08.9TDLSB-A.L1-5.
[168] Neste sentido, CARDOSO – *RMP*. Ano 39. N.º 153 (jan -mar 2018), p. 170 e 191 e 214.
[169] *Idem*, p. 191.

A danosidade social e jurídica do acesso à correspondência, dita tradicional, acaba por ser menor do que a do acesso ao correio eletrónico. O espetro de danosidade e de pessoas envolvidas cuja troca de comunicações é conhecida e revelada é maior no correio eletrónico. Ainda assim, estabeleceu-se um regime menos restritivo, embora, mais exigente, em certos aspetos, capaz de corresponder às exigências da nova criminalidade, da nova forma de investigação criminal, da atual atividade probatória e que não a inviabilize.

Remetendo-se para o regime da apreensão de correspondência sem esclarecer em que termos e condições, levanta-se a questão de saber qual é a extensão da remissão para o artigo 179.º do CPP.

Adiantamos, desde já, que, quanto aos requisitos previstos no n.º 1 do artigo 179.º do CPP, consideramos que apenas vigora para a apreensão de correio eletrónico a alínea c). Não existe distinção entre correio eletrónico aberto e fechado[170] e o catálogo de crimes aplicável é o que se encontra previsto no artigo 11.º da LC. Não se prescinde, portanto, do grande interesse para a descoberta da verdade ou para a prova.

Com base nesta interpretação, podemos adiantar que a remissão para o artigo 179.º do CPP não é uma remissão *tout court*, existindo diferenças entre os dois métodos de obtenção de prova que acabam por se repercutir no regime de cada um e que fragilizam esta remissão e equiparação.

Quanto ao n.º 2 do artigo 179.º do CPP consideramos, sem qualquer dúvida, que o mesmo se aplica à apreensão de mensagens de correio eletrónico, o que significa que, no caso de a correspondência se encontrar abrangida pelo regime do segredo, este irá sempre prevalecer, salvo se puder ser levantado nos casos, expressamente, previstos na lei.

Questões mais controversas e que, por essa razão, consideramos merecerem um tratamento autónomo e mais aprofundado, são as que respeitam à exigência de despacho

[170] A doutrina e a jurisprudência têm interpretado o artigo 179.º do CPP no sentido de este dever ser aplicado à correspondência em trânsito ou ainda não aberta, enquanto a correspondência já aberta deverá ser submetida ao regime geral do artigo 178.º do CPP. Quando olhamos para o artigo 17.º da LC verificamos que, por um lado, não se refere ao correio eletrónico "em trânsito", pois neste casso, estaria em causa uma interceção em tempo real, pelo que deverá ser aplicado o artigo 18.º da LC. Por outro lado, não há qualquer referência a mensagens abertas e fechadas. Deste modo, como já defendemos *supra*, a lei não estabelece qualquer distinção apenas se referindo a mensagens armazenadas num sistema informático.

de autorização ou ordem do JIC para a apreensão e o conhecimento, em primeiro lugar, das mensagens apreendidas pelo JIC.

1.3.1. A exigência da autorização ou ordem judicial prévia

Adotamos uma interpretação literal e sistemática[171], do artigo 17.º da LC, que tem em consideração a referência à expressão "autorizar ou ordenar", para a fase do inquérito e a para as restantes fases do processo, respetivamente. Consideramos, por isso, que a apreensão de mensagens de correio eletrónio tem de ser, obrigatoriamente, autorizada pelo JIC, na fase de inquérito, uma vez que o titular do processo, nesta fase, é o MP e ordenada pelo juiz competente, nas restantes fases do processo.[172]

Esta interpretação pode gerar alguns problemas, na prática, quanto à boa prossecução da investigação. Por um lado, porque, indiretamente, vai fazer depender a pesquisa de dados informáticos, neste caso de dados de conteúdo, do despacho do JIC e não da autoridade judiciária, como se estabelece no artigo 15.º da LC. Por outro lado, porque pode tornar inviável a apreensão das mensagens de correio eletrónico, caso estas sejam encontradas no decurso de uma busca ou pesquisa em sistema informático e não exista um despacho do JIC de autorização ou ordem da sua apreensão.

Uma outra interpretação pode definir que o sentido da expressão, "autorizar" pode significar que este ato de autorização é posterior a uma primeira apreensão formal.

---

[171] Em todos os casos em que se usa a expressão "autorizar e ordenar", está presente a distinção das fases processuais em que o juiz intervém, autorizar na fase de inquérito, em que o *dominus* do processo é o MP e ordenar, nas restantes fases do processo, quando é o juiz o *dominus* do processo.

[172] Cfr. TRG – Acórdão de 15 de outubro de 2012, processo n.º 68/10.1GCBRG.G1: "tal intervenção impõe-se apenas quando os dados pretendidos não estão acessíveis, quando não são espontaneamente fornecidos por quem pode dispor deles livremente.
Só nesses casos é obrigatória a intervenção do juiz de instrução, que terá de ponderar e decidir qual dos valores conflituantes deverá prevalecer: o respeito pela reserva da vida privada, ou o interesse da administração da justiça.". Só assim, atribuindo-se ao juiz das liberdades e garantias poderes para decidir, se pode considerar respeitada a *mens legislatoris* e a coerência do sistrema. Decisão essa que tem de refletir uma ponderação dos interesses em causa, subordinada ao princípio da proporcionalidade, nas suas três vertentes, proporcionalidade em sentido estrito, adequação e subsidiariedade. Neste sentido, TRC – Acórdão de 4 de fevereiro de 2015, processo n.º 73/14.9JALRA-A.C1.
TRP- Acórdão de 3 de abril de 2013, processo n.º 856/11.1PASJM.P1, o tribunal fundamenta a sua decisão no n.º3 do artigo 15.º da LC, o que significa que *a contrario*, ou seja, não existindo consentimento por parte do titular do bem jurídico, a apreensão depende de autorização judicial, de acordo com o artigo 17.º da LC. Quanto à obrigatoriedade de autorização judicial para junção aos autos *vide* TRP – Acórdão de 13 de abril de 2016.

Admite, por isso, a possibilidade de existir uma apreensão cautelar[173], que não depende de prévia autorização ou ordem judicial[174] e que será, posteriormente, autorizada ou validada pelo JIC.[175]

Nesta perspetiva, o despacho do juiz poderá ser posterior ao conhecimento da existência de mensagens de correio eletrónico e à sua apreensão por parte de quem está a realizar a busca e a pesquisa[176], pois considera-se que só assim haverá algo a apresentar ao juiz[177].

Argumenta-se no sentido de que como o pedido de apreensão é da iniciativa do MP, será também dele a seleção das comunicações cuja apreensão se autorizará ou não e que caso assim não fosse, nunca existiria uma verdadeira autorização do JIC, mas sim, sempre, uma decisão de ordem.[178]

Acrescenta-se ainda que o MP não pode requerer a apreensão de mensagens de correio eletrónico que se afigurem de grande interesse para a descoberta da verdade ou para a prova se não as conhecer.[179]

Considera-se que "se fosse intenção do legislador aplicar integralmente o regime da apreensão do CPP, bastar-lhe-ia ter dito que à apreensão das mensagens de correio eletrónico é aplicável o regime da apreensão de correspondência previsto no CPP"[180].

Todavia, não concordamos com o presente argumento, uma vez que quanto a esta questão, não há remissão para o regime da correspondência, é a própria previsão

[173] Neste sentido VERDELHO – *Scientia*, T. LVIII. N.º 320 (out.- dez. 2009), p. 743.
[174] Neste sentido (quanto à apreensão de correspondência), TRC – Acórdão de 7 de junho de 2017, processo n.º 96/14.8EALSB-A.C1.
[175] Este argumento coincide com a interpretação do artigo 179.º do CPP no sentido de que o JIC tem de ordenar para valer como prova e não para apreender.
[176] Quanto a esta questão TRG – Acórdão de 29 de março de 2011, processo n.º 735/10.0GAPTL – A.G1, na parte em que refere o recurso apresentado pelo MP: o JIC considerou que o MP é quem deve tomar conhecimento em primeira mão decidindo quais se afiguram uteis à produção de prova e interessam para a descoberta da verdade material. Caso considere relevante, apreende, provisoriamente, apresentando-as ao JIC, que caso o entenda, ordena a apreensão definitiva, juntando-as ao processo nos termos dos artigos 17.º e 16.º n.º 3 da LC. O MP não entendeu assim, dizendo que deve ser da competência do JIC a apreciação da apreensão provisoria levada a cabo pelo MP em ordem a ordenar ou não a junção aos autos da prova recolhida no telemóvel nos termos dos artigos 17.º e 16.º n.º 3 da LC e do artigo 179.º n.º 3, 2.ª parte, do CPP.
[177] CARDOSO – *RMP*. Ano 39. N.º 153 (jan -mar 2018), p. 179.
[178] Neste sentido, *idem*, p. 196.
[179] *Idem*, p. 197.
[180] *Idem*, p. 195.

normativa do artigo 17.º da LC que estabelece que a apreensão tem de ser autorizada ou ordenada pelo juiz.

Em coerência com a letra da lei e com a ordem sistemática do CPP que utiliza, em todo o CCP, a expressão "autorizar" para a fase de inquérito e a expressão "ordenar" para as restantes fases do processo, consideramos que para se poder realizar a apreensão de mensagens de correio eletrónico, terá de existir um despacho prévio do JIC que autorize ou ordene a referida diligência.

Reconhecemos que esta interpretação pode implicar algumas consequências que dificultem o decurso da investigação, mas não podemos deturpar a letra da lei e o que nela se estabelece em função daquilo que se nos afigura ser o que deveria existir.

Com base na interpretação que não defendemos, retirar-se-ia do texto da norma que, "a única exigência legal para a sua apreensão provisória é a da existência de uma forma legítima de acesso ao meio informático em que as mensagens estavam armazenadas"[181].

Segundo este entendimento, após a apreensão formal das mensagens, se o juiz entender que as mensagens consubstanciam prova relevante para o processo, este deve proceder à autorização ou ordem da apreensão e só nesse momento é que a mensagem será, efetivamente, apreendida e junta ao processo.

De forma inversa, se o juiz considerar que as mensagens não apresentam relevância ou interesse para o processo, a apreensão não se mantém pelo que deve permitir-se novamente o acesso ao sistema informático[182] por parte do visado. O suporte informático onde foram encontradas deverá ser devolvido[183].

Esta interpretação acaba por flexibilizar o regime no sentido de facilitar o decurso da própria investigação, não fazendo depender a apreensão cautelar da prévia intervenção do juiz.

[181] VERDELHO – *Scientia*, T. LVIII. N.º 320 (out.- dez. 2009), p. 743.
[182] O sistema informático a que nos referimos é a conta de correio eletrónico e não necessariamente o dispositivo físico, *v.g.* computador ou telemóvel, apreendido, uma vez que podem existir mais provas nesse mesmo sistema que ainda possam ser apreendidas. Caso não existam, o dispostito deverá também ser devolvido.
[183] No caso de a apreensão se processar através de cópia, a mesma deverá ser destruída.

Quem admite a possibilidade de uma apreensão provisória sem despacho judicial considera que é inviável que, antes de qualquer busca, quando ainda não se sabe se se encontrará um sistema informático e se nesse sistema informático se encontrarão mensagens de correio eletrónico relevantes para o processo, se exija a intervenção do juiz para autorizar ou ordenar a apreensão de mensagens.[184]

Significa, portanto, segundo esta linha de entendimento, que apenas a junção das mensagens de correio eletrónico ao processo tem de ser autorizada ou ordenada pelo juiz, ou seja, este apenas valida a junção das mensagens para efeitos de prova.

Baseia-se esta interpretação no n.º 3 do artigo 16.º da LC, uma vez que as mensagens de correio eletrónico, no fundo, mais não são do que dados de conteúdo[185], que refere que o JIC pondera em relação à junção e não quanto à apreensão.

Entendendo que a remissão, em bloco, para o 179.º do CPP não faz sentido e para tornar mais viável a apreensão, não a fazendo depender, *a priori*, da autorização ou ordem do JIC, poderíamos recorrer ao n.º 3 do artigo 16.º da LC, tendo em conta que apreensão da mensagem de correio eletrónico é um caso especial de apreensão de dados de conteúdo.

A dependência de autorização ou ordem judicial prévia pode, em certos casos, causar alguns entraves ao decurso da investigação. Todavia, a adoção desta interpretação poderá levar a um afastamento face ao regime da apreensão previsto na LC, onde a lei impõe de forma expressa a exigência de despacho do JIC para a apreensão, não se referindo à junção, como o faz no n.º 3 do seu artigo 16.º. Tem de existir um despacho judicial para que as mensagens de correio eletrónico possam ser apreendidas.

O recurso ao n.º 3 do artigo 16.º da LC é uma opção facilitadora da aplicação do regime na prática. Porém, se atentarmos na letra do artigo 17.º da LC que regula a apreensão de dados de conteúdo de carácter especial, as mensagens de correio eletrónico, consideramos que o despacho do JIC respeita à apreensão da mensagem.

Ainda que tenhamos consciência de que a nossa interpretação poderá, em alguns casos, inviabilizar a investigação, prezamos o respeito e o cumprimento da letra da lei, bem como a proteção dos direitos fundamentais que se visam proteger. Consideramos, por

[184] Cfr. VERDELHO – *Scientia*, T. LVIII. N.º 320 (out.- dez. 2009), p. 744.
[185] Embora, com uma proteção acrescida, o que pode fazer a diferença.

isso, que esta interpretação é a que menos margem deixa para derivações e incumprimentos do regime.

1.3.2. O conhecimento, em primeiro lugar, pelo JIC

Quanto ao conhecimento das mensagens de correio eletrónico após a sua apreensão, o artigo 17.º da LC é completamente omisso, restando apenas o que se prevê no regime da apreensão de correspondência, por via da remissão.

No n.º 3 do artigo 179.º do CPP estabelece-se que o juiz deve ser o primeiro a ter conhecimento do conteúdo das mensagens, delas decidindo sobre a sua relevância para o processo, *maxime*, para a descoberta da verdade.

A alínea d) do n.º 1 do artigo 268.º do CPP, atribui também competência exclusiva ao JIC para tomar conhecimento, em primeiro lugar, do conteúdo da correspondência apreendida.[186]

"O exame da correspondência pelo juiz é um acto legalmente obrigatório, pelo que a sua omissão pelo Mmo. J.I.C. constitui uma nulidade prevista no art. 120.º n.º 2 al. d) do Cód. Proc. Penal."[187]

Sobre esta questão, podemos apreciar também o Acórdão do Tribunal da Relação de Lisboa de 11 de janeiro de 2011, processo n.º 5412/08.9TDLSB-A.L1-5[188], que vem neste mesmo sentido, anulando o despacho do JIC que determinou que não há obrigatoriedade de este ser o primeiro a tomar conhecimento do correio eletrónico, mas apenas "de um juízo sobre a necessidade e proporcionalidade da efetiva apreensão das mensagens"[189].

---

[186] *Vide* TRL – Acórdão de 6 de fevereiro de 2018, processo n.º 1950/17.0 T9LSB-A.L1-5.

[187] TRL – Acórdão de 20 de dezembro de 2011, processo n.º 36/11.6PJOER-A.L1-5, que refere, ainda, que, "Constituindo a leitura da correspondência um atentado ao direito da inviolabilidade da mesma, só o juiz de instrução criminal pode, verificando-se os requisitos legais, determinar a apreensão de correspondência, validar a apreensão de correspondência, ser a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, e, ser quem decide se a mesma é ou não relevante."

[188] "Não se vê igualmente, que face às exigências constantes do regime legal, que exige despacho do JIC e que este seja a pessoa a tomar conhecimento "em primeiro lugar" do conteúdo da correspondência e do correio electrónico apreendidos, "sob pena de nulidade", que se pudesse entender, como no despacho recorrido, que se criara um regime legal dito "específico", diverso, menos exigente, e que pudesse dispensar o cumprimento do disposto no art.º 179º nº 3 do CPP, quando os termos da lei especial, Lei do Cibercrime, (Lei nº 109/2009, de 15 de Setembro,) remetem expressamente para o regime geral previsto no Código de Processo Penal, sem redução do seu âmbito, antes se impondo a sua aplicação na sua totalidade, termos em que se concederá provimento ao recurso.".

[189] TRL – Acórdão de 11 de janeiro de 2011, processo n.º 5412/08.9TDLSB-A.L1-5.

No seguimento do que foi dito a propósito da apreensão provisória vêm os mesmos autores afirmar que o juiz não será a primeira pessoa a tomar conhecimento do teor das mensagens. Quem procede à pesquisa do sistema informático e encontra mensagens, que decide levar ao JIC, toma conhecimento do teor das mesmas e apenas leva ao conhecimento do JIC mensagens concretas, com relevância para o caso concreto que depois poderão ou não ser apreendidas.[190]

Novamente, o argumento é o da inviabilidade, no sentido em que seria impossível que um único juiz verificasse todas as mensagens de correio eletrónico, recebidas e enviadas de todos os computadores, principalmente, quando estão em causa investigações de criminalidade altamente organizada ou da qual façam parte pessoas coletivas, em que o volume de mensagens enviadas e recebidas poderá ser muito elevado.

Argumenta-se, ainda, no sentido de existir uma incoerência na tutela de direitos, verificando-se uma menor tutela em situações que podem ser potencialmente mais lesivas de direitos fundamentais. Refere-se, por um lado, as possíveis restrições com maior gravidade para a privacidade presentes nos artigos 16.º, n.º 3 e 18.º da LC em que o MP pode e deve tomar conhecimento, em primeiro lugar, do conteúdo. Por outro lado, aos casos menos graves como a apreensão de mensagens de correio eletrónico em que pode nem sequer existir uma violação da privacidade em que deve ser o JIC o primeiro a tomar conhecimento.[191]

Podemos até reconhecer que pode verificar-se uma certa incoerência. O regime de interceção de comunicações em tempo real não impõe que o JIC seja o primeiro a tomar conhecimento do conteúdo das mesmas, pelo contrário verifica-se que pode existir um conhecimento prévio pelos OPC, nos termos do artigo 188.º do CPP. Contudo, ao remeter-se para o regime da correspondência, esta exigência terá de ser cumprida, sob pena de nulidade, caso contrário ter-se-ia mantido a remissão para o regime das escutas telefónicas, que vigorou até 2009. A mudança de paradigma gerada pela LC não pode ser

[190] Neste sentido, VERDELHO – *Scientia*, T. LVIII. N.º 320 (out.- dez. 2009), p.744 e no mesmo sentido, TRL – Acórdão de 2 de março de 2011, processo n.º, entendeu ainda que no âmbito de troca de correspondência entre arguido e defensor, que a correspondência depois de aberta não merece a tutela do sigilo da correspondência, tendo um voto de vencido no sentido de que a proibição do n.º 3 visa tutelar as garantias do arguido, direito à privacidade.
[191] Neste sentido, CARDOSO - *RMP*. Ano 39. N.º 153 (jan -mar 2018), p. 198.

ignorada e muito menos afastada ou derrogada apenas devido ao argumento da incoerência normativa.

Deve cumprir-se o que foi estabelecido pela lei e respeitar a sistematicidade e a proteção atribuída aos direitos em causa. Podemos discordar, fazer uma análise critica e defender outra solução que consideramos ser a mais adequada, não obstante, tal não pode traduzir-se no incumprimento do que está estabelecido na lei e na aplicação de um outro regime que não o que nela se encontra previsto.

"Na apreensão de correspondência, a obrigatoriedade de ser o juiz a tomar conhecimento do conteúdo da correspondência visa assegurar que o conteúdo da correspondência estava efectivamente nela contida. Não é para impedir que outros que não o juiz tomem conhecimento do conteúdo dessa correspondência em caso de irrelevância probatória"[192].

Ainda assim, também na apreensão de mensagens de correio eletrónico, o primeiro conhecimento pelo JIC visa assegurar que não existe qualquer alteração ou eliminação dos dados informáticos[193].

Potencializa-se uma maior dispersão do conteúdo, aumentando as probabilidades de fuga de informação ou de adulteração e destruição de prova.

Assim como a extensão do âmbito da tutela das comunicações ao conteúdo da mensagem, mesmo quando o ato comunicacional, em sentido estrito, já cessou, visa a sua proteção, evitando uma abusiva ingerência nas comunicações, também o requisito do conhecimento, em primeiro lugar, pelo JIC tem o mesmo intuito.

O facto de não ser o JIC a tomar o primeiro conhecimento e a decidir da junção das mensagens que se mostram relevantes para o processo causa uma maior invasão na privacidade e, em consequência, uma maior restrição e lesão dos direitos fundamentais que se visam proteger.

[192] CARDOSO – *RMP*. Ano 39. N.º 153 (jan -mar 2018), p. 202.
[193] Evitando, desta forma, que possam ser enviadas mensagens em nome do titular da conta mas não da sua autoria ou eliminadas outras mensagens que possam adquirir grande interesse para a descoberta da verdade e da prova.

Tendo em consideração os deveres de independência e imparcialidade do JIC, enquanto juiz das liberdades e das garantias, consideramos que deve ser este a ter o primeiro controlo na apreensão e na leitura das mensagens.

Qualquer ingerência no correio eletrónico que não cumpra os requisitos legalmente previstos corresponderá a prova nula e proibida, nos termos dos artigos 32.º n.º 8 da CRP e 120.º, n.º 2, al. d), 125.º e 126.º n.º 1 e n.º 3 do CPP.

No que respeita às regras de procedimento, existe uma remissão expressa "para o regime geral previsto no Código de Processo Penal, sem redução do seu âmbito, antes se impondo a sua aplicação na sua totalidade"[194], para o que não está expressamente regulado na LC e no que não lhe seja contrário.

1.4. O artigo 189.º do CPP

Tem-se entendido que a LC procedeu à revogação[195] tácita e parcial do artigo 189.º do CPP, na parte em que se refere às comunicações por meio diferente de telefone, especificamente, quanto à apreensão destas quando armazenadas em suporte digital.

Todavia, várias têm sido as alterações ao CPP onde se tem ignorado esta questão, mantendo, a totalidade do seu texto.

Embora se considere que a entrada em vigor da LC veio estabelecer um novo regime de apreensão de correio eletrónico, podemos questionar-nos se poderá fazer sentido remeter-se, ainda, para o artigo 189.º do CPP para suprir uma eventual lacuna relativamente à aplicação do regime da correspondência, que irá inviabilizar a norma legal e a investigação. Referimo-nos, portanto, ao n.º 3 do artigo 179.º do CPP e da sua inexequibilidade quanto à realidade atinente à apreensão de mensagens de correio eletrónico.

Na fase de inquérito é o MP o *dominus* do processo pelo que fazer depender esta diligência do JIC, sem qualquer intervenção do MP pode ser um pouco contraditório com a atribuição da direção do inquérito ao MP.[196]

[194] TRL – Acórdão de 6 de fevereiro de 2018, processo n.º 1950/17.0 T9LSB-A.L1-5.
[195] Com base no princípio *lex posteriori derogat priori*.
[196] Todavia, ainda que a direção do inquérito caiba ao MP, existem atos que são da exclusiva competência do JIC, por via dos artigos 268.º e 269.º do CPP.

Podemos admitir que existem, neste caso, dois filtros formais quanto ao controlo da prova. Há um primeiro controlo efetuado pelo MP ou pelo OPC e, posteriormente, um segundo controlo pelo JIC que decidirá da junção aos autos do que considera relevante para a prova.

Em abono desta solução, pode afirmar-se que esta se mostra bem mais compatível com a realidade digital. Reconhecemos que pode não ser exequível que numa apreensão de milhares de mensagens de correio eletrónico seja o JIC a tomar conhecimento, em primeiro lugar, de todas essas mensagens, quando nem sequer é ele o *dominus* do processo[197], podendo atuar sem qualquer intervenção do MP.

Ora, o lugar paralelo, onde podemos encontrar uma solução que seja algo garantística e que não inviabilize a investigação será o artigo 189.º do CPP que remete para o artigo 187.º do mesmo diploma legal e, com base nesta interpretação, legitimar que possa ser o MP ou o OPC a tomar conhecimento, em primeiro lugar, das mensagens.

É uma opção que, aparentemente, facilita o decurso do processo do ponto de vista prático, uma vez que não cai apenas sobre uma única pessoa, o JIC, o conhecimento de todas as mensagens recebidas e enviadas através daquele sistema informático. Todavia, cria alguns problemas, quer do ponto de vista sistemático, quer em termos de segurança e estabilidade jurídica, bem como no que respeita à proteção de direitos fundamentais.

Várias foram as oportunidades para reformular ou mesmo revogar o artigo 189.º do CPP, todavia este continua inalterado e, por isso, poderíamos questionar, qual a razão da sua redação, tal como está, após a entrada em vigor da LC.

Contudo, não cremos que, quanto à apreensão de mensagens de correio o artigo, 189.º do CPP ainda seja aplicável, por via do princípio *lex posteriori derogat priori*. Desta forma, remete-se para o regime da correspondência a apreensão de mensagens de correio eletrónico, quando o ato comunicacional, em sentido estrito, já cessou, e para o regime das escutas telefónicas a interceção real deste meio de comunicação.

[197] Embora seja, ele, o juiz das liberdades e das garantias.

1.5. A apreensão de correio eletrónico no telemóvel

No que respeita à apreensão de mensagens de correio eletrónico armazenadas e acessíveis num telemóvel podem surgir algumas dúvidas relativamente ao regime aplicável.

Por um lado, tem-se entendido que o telemóvel corresponde não a um meio técnico diferente do telefone, mas sim a um telefone pelo que não poderá considerar-se abrangido pela extensão do artigo 189.º do CPP. A apreensão de *SMS* ou de quaisquer outras comunicações (já terminadas) neste dispositivo deve, portanto, ser realizada ao abrigo do regime da correspondência previsto no artigo 179.º do CPP.[198]

Por outro lado, contrariamente ao descrito *supra*, poderia considerar-se que o telemóvel estaria abrangido pelo artigo 189.º do CPP e que, por ser um sistema de telecomunicações, qualquer diligência que tenha como objeto este dispositivo deve ser realizada de acordo com o previsto no referido artigo. Esta posição adota uma solução mais prudente e garantística, em termos de risco processual[199], sujeitando a apreensão de mensagens de correio eletrónico no telemóvel ao regime das escutas telefónicas.

Este entendimento pode criar algumas assimetrias. Deste modo, se o acesso à mesma informação se realizar através de um telemóvel será muito mais restritivo do que se for através de um computador.

Por fim, há, ainda, o entendimento de que os telemóveis, conquanto tenham sido e ainda possam ser considerados, em parte, sistemas de telecomunicações, atualmente, são constituídos por sistemas informáticos tão ou mais complexos que os computadores. O envio de *SMS* e, principalmente, de mensagens de correio eletrónico realiza-se através do sistema informático.

[198] Neste sentido, TRP – Acórdãos de 27 de janeiro de 2010, processo n.º 896/07.5JAPRT.P1 e de 12 de setembro de 2012, processo n.º 787/11.5PWPRT.P1.
[199] Para evitar uma possível anulação da prova, por cautela, dever-se-ia aplicar o regime das escutas, pois o que aqui estaria em causa seria um sistema de telecomunicações.

O artigo 17.º da LC não estabelece qualquer distinção em função do aparelho que é utilizado para realizar a comunicação apenas se refere a sistemas informáticos, onde consideramos que os telemóveis se integram.[200]

Como já referimos deve estabelecer-se a distinção entre a interceção de comunicações em tempo real, aplicando-se o regime dos artigos 18.º da LC e 187.º e 188.º do CPP e a apreensão do conteúdo resultante da comunicação, aplicando-se o regime dos artigos 17.º da LC e 179.º do CPP.

A aplicação de regimes distintos em função do dispositivo onde se encontram armazenadas as mensagens pode tornar-se inexequível.

Este entendimento só poderá fazer sentido se todas as mensagens tiverem sido enviadas e recebidas através do telemóvel, caso contrário já não está em causa uma comunicação realizada através do telemóvel enquanto sistema de telecomunicações.

Da mesma forma, na apreensão de mensagens de correio eletrónico através de um computador, só poderiam ser alvo de apreensão as mensagens enviadas e recebidas através do mesmo, pois se alguma mensagem tivesse sido enviada ou recebida através de um telemóvel tal já constituiria uma comunicação através de um sistema de telecomunicações e, portanto, teria de se aplicar o artigo 189.º do CPP.

Ora, parece-nos que tal distinção seria impossível e poderia tornar inviável a utilização deste meio de obtenção de prova.

Compreendemos a prudência na defesa desta orientação, mas não consideramos que tal se possa retirar da letra da lei, nem da proteção que esta consagra.

1.6. Conclusões

"O carácter assistemático destas intervenções legislativas criou uma total inconsistência no sistema dos meios de obtenção de prova, havendo actualmente objectos de registos da palavra escrita (telegrama, fax, telex) sujeitos ao regime geral das apreensões (artigo 178.º) quando o seu conteúdo é conhecido pelo seu destinatário e

[200] Neste sentido, TRG – Acórdão de 29 de março de 2011, processo n.º 735/10.0GAPTL – A.G1, TRL – Acórdão de 24 de setembro de 2013, processo n.º 145/10.9GEALM.L2-5 e TRP – Acórdão de 3 de abril de 2013, processo n.º 856/11.1PASJM.P1.

sujeitos a um regime especial de apreensão (art.179.º) quando o seu conteúdo é ainda desconhecido pelo seu destinatário e ainda objetos de registo da palavra escrita (os referidos suportes materiais de correio electrónico ou de outras formas de transmissão de dados por via telemática) submetidos ao regime das escutas telefónicas, independentemente do seu conteúdo ser já conhecido ou não pelo destinatário"[201].

A LC trouxe, por um lado, a previsão de novos meios de obtenção de prova, mas, por outro, implicou a alteração de regimes já existentes, o que levou, ainda que de forma não expressa e clara, à revogação dos mesmos, criando problemas de interpretação e de aplicação de um regime uniforme.

Quanto à apreensão de correio eletrónico, deixa de se remeter para o regime do artigo 189.º, n.º 1 do CPP, passa a remeter-se para o regime do artigo 179.º do CPP, alarga-se o âmbito de aplicação, amplia-se o catálogo de crimes e facilita-se a obtenção deste meio de prova, cada vez mais relevante para a investigação criminal e para a atividade probatória.

O artigo 17.º da LC manteve a referência às mensagens armazenadas em suporte digital, independentemente do seu estado, que continua a ser ignorada tanto pela doutrina como pela jurisprudência.

Consideramos, por isso, que, ainda que o artigo 17.º remeta para o regime da correspondência, o mesmo deve aplicar-se independentemente de as mensagens se encontrarem abertas ou fechadas.

Na verdade, os grandes pontos da discussão são a dependência ou não de autorização ou ordem judicial para proceder à apreensão das mensagens e a exigência de o JIC ser o primeiro a tomar conhecimento do conteúdo das mesmas.

Podemos até compreender que, para quem participa na investigação e realiza estas diligências, a ausência destas exigências acaba por facilitar e agilizar a própria investigação e obtenção deste meio de prova.

[201] PINTO DE ALBUQUERQUE – *Comentário*, p. 542.

Contudo, não cremos que seja essa a solução que se retira da letra da lei, nem da proteção atribuída às comunicações.

Tendemos a concordar com a opinião de quem defende que se negligenciou, mais uma vez, as necessidades de criação de um regime específico, detalhado e esclarecido que tenha em consideração as especificidades deste meio de comunicação.[202]

Desordem legislativa que ainda é mais evidente quando estão em causa comunicações realizadas através de sistemas informáticos que são ao mesmo tempo sistemas de telecomunicações, quer sejam mensagens de correio eletrónico ou "comunicações de natureza semelhante" abrangidas pelo artigo 17.º da LC, onde podemos incluir as *SMS*, que também têm sido abrangidas pelo n.º 1 do artigo 189.º do CPP, na parte que ainda não se encontra revogada, ou mesmo diretamente pelo regime da correspondência, previsto no artigo 179.º do CPP.

No que respeita à interpretação do artigo 17.º da LC, privilegiamos uma interpretação literal, em que a letra da lei funciona como ponto de partida e como limite da interpretação, mas que também encontra apoio noutros elementos.

Quanto ao elemento racional, este compreende, em primeiro lugar, a *ratio legis* da presente norma. Por um lado, visa permitir a possibilidade de utilização deste meio de obtenção de prova na investigação de um maior número de crimes, uma vez que o catálogo aplicável é mais amplo do que o previsto no regime anterior. Por outro lado, visa proteger a ingerência e o sigilo nas comunicações, tendo em conta a natureza privada do seu conteúdo, evitando a devassa por terceiros, a dispersão do seu conteúdo e, em consequência, uma maior invasão na privacidade.

Em segundo lugar, as razões políticas, sociais e económicas que correspondem, no fundo, à "conjetura politico-económico-social"[203] (*occasio legis*), que levaram à criação da LC e, especificamente, à criação do seu artigo 17.º.

A expansão dos meios de comunicação eletrónicos acabou por potencializar a criminalidade informática e a criminalidade praticada através destes meios. A prova

[202] DÁ MESQUITA – *Processo Penal*, p. 118 e 119.
[203] MACHADO, João Baptista – *Introdução ao Direito e ao Discurso Legitimador*. 17.ª Reimpressão. Coimbra: Almedina, 2008. p.182.

essencial para a investigação deste tipo de criminalidade encontra-se em suportes informáticos cuja obtenção reivindica novos meios de obtenção de prova, bem como a adequação dos já existentes a esta nova realidade.

O artigo 17.º da LC surge, na sequência da Lei da Criminalidade Informática e da ratificação da Convenção sobre o Cibercrime, como mais uma resposta a estes novos desafios, fornecendo ao sistema processual penal atual normas que permitem a obtenção de prova digital.

O elemento sistemático compreende uma interpretação "em consonância com a unidade intrínseca de todo o ordenamento jurídico"[204] que nos permite sustentar a interpretação segundo a qual a expressão "autorizar ou ordenar" é utilizada para diferenciar a atuação do juiz nas diferentes fases do processo, autorizar para a fase de inquérito e ordenar para as restantes fases do processo. Além deste aspeto, importa atentar na proteção constitucional das comunicações, cuja ingerência só é permitida no âmbito penal, dentro dos parâmetros estabelecidos pela lei.

Por fim, o elemento histórico que, embora o instituto seja algo recente, permite concluir que o regime é atualmente mais amplo do que o anterior, apresentando, em alguns aspetos, requisitos mais exigentes na sua obtenção. Visa-se uma maior facilidade de acesso e obtenção deste meio de prova que se mostra, cada vez mais, indispensável na investigação, impedindo, todavia, que essa facilidade se transforme numa ingerência abusiva e incontrolada nas comunicações.

[204] BAPTISTA MACHADO – *Introdução*, p. 183

2. O consentimento do visado: alcance e limites

No que ao acesso ao correio eletrónico diz respeito, entendemos por consentimento a permissão por parte do visado, para se aceder à sua conta de correio eletrónico.

Permissão que tem de refletir uma manifestação de vontade livre e esclarecida que demonstre que o visado concorda e autoriza que a diligência seja praticada.

Se no decurso de uma busca ou numa pesquisa a sistema informático, as autoridades não dispuserem de um despacho do JIC que autorize ou ordene a apreensão das mensagens de correio eletrónico, a mesma estará dependente da vontade do visado. Neste caso, para que o consentimento seja válido, as autoridades que procedem às diligências devem prestar todas as informações que permitam ao visado perceber no que consiste e quais as consequências do seu consentimento.

O consentimento tem de demonstrar que o visado compreendeu e permite que as autoridades acedam à sua conta de correio eletrónico para procederem à apreensão das mensagens nela constantes.

A apreensão de correio eletrónico tanto pode compreender as mensagens recebidas como as enviadas pelo visado. Considera-se, portanto, que o destinatário, ao receber a mensagem, ainda que esta não seja da sua autoria, passa a ter total disponibilidade sobre a mesma.

Importa, agora, determinar quem é o visado, isto é, no fundo, quem é o titular do direito, que pode ser alvo de uma apreensão e, em consequência, de uma ingerência nas suas comunicações.

O visado pode ser o suspeito da prática de um crime, a vítima, ou ainda um terceiro[205] "se houver razões para suspeitar de que ele saiba que a sua correspondência está a ser utilizada pelo visado para um fim ilícito"[206] ou mesmo "em relação ao qual não houver razões para suspeitar que ele saiba que o seu correio está a ser utilizado pelo visado para um fim ilícito"[207].

[205] Diferente do visado inicial, mas que passará a ser também visado.
[206] PINTO DE ALBUQUERQUE – *Comentário*, p. 509.
[207] *Ibidem.*

Não é, portanto, necessária a constituição de arguido, para que se possa proceder à apreensão de correio eletrónico, bastando o cumprimento dos requisitos legais *supra* referidos.

Para que as autoridades judiciárias possam aceder à conta de correio eletrónico para procederem à apreensão das respetivas mensagens necessitam que o visado lhes dê acesso à respetiva conta, revelando a palavra-passe. Neste caso, estar-se-á perante uma situação de consentimento. Caso tal não se verifique, terão de estar munidos de uma autorização ou ordem judicial e, posteriormente, pedir autorização ao servidor para que o acesso seja feito de forma legal.

2.1. O direito ao silêncio e o privilégio contra autoincriminação

Como já referimos, o visado não tem de ser, necessariamente, arguido, mas no caso de ser, coloca-se a questão de saber se este pode ser obrigado a revelar a palavra-passe de acesso ao sistema informático e à conta de correio eletrónico.

"O visado/arguido pelo processo conserva plenamente o seu direito de defesa relativamente às informações confidenciais que sejam de uma forma ou de outra como meio de prova no processo"[208]. A defesa do arguido, numa primeira ponderação de interesses, deve prevalecer, "aliás, outra solução seria inconstitucional por direta e flagrante violação do artigo 32.º, n.º 10, da Constituição, segundo a qual "nos processos de contra-ordenação, bem como em quaisquer processos sancionatórios, são assegurados ao arguido os direitos de audiência e de defesa"[209].

No fundo, importa saber se vigora, através do direito ao silêncio, a proteção conferida pelo privilégio contra a autoincriminação que determina que nenhum arguido tem o dever de participar ou colaborar com a justiça, quando tal implique a sua colocação perante uma situação incriminatória.

[208] MOUTINHO, José Lobo – "Comentário ao Artigo 31.º – Prova". In PORTO, Lopes Manuel; VILAÇA, José da Cruz; CUNHA, Carolina; HENRIQUES, Miguel Gorjão; ANASTÁCIO, Gonçalo (Coord.). HENRIQUES, Miguel, Gorjão (Dir.) – *Lei da Concorrência – Comentário Conimbricense.* Coimbra: Almedina, 2013. p. 334. Embora seja referente ao direito das contraordenações no domínio do direito da concorrência, consideramos que tal também se aplica ao processo penal nos termos gerais.
[209] *Idem*, p. 335.

Existe, todavia, alguma confusão semântica e jurídica, entre o direito ao silêncio e a garantia contra a autoincriminação.

Não há uma consagração constitucional expressa do privilégio contra a autoincriminação nem do direito ao silêncio.

No entanto, o CPP, no seu artigo 61.º, n.º 1, alínea d), estabelece o direito ao silêncio do arguido, consagrando, desta forma, também uma garantia contra a autoincriminação.

O facto de não existir uma consagração expressa na Constituição, quer do privilégio contra a autoincriminação, quer do direito ao silêncio não significa que estes não tenham relevância constitucional, uma vez que acaba por se integrar no âmbito de proteção do direito de defesa, presente no artigo 32.º, nº 1 da CRP[210].

O privilégio contra a autoincriminação tem um âmbito mais amplo, ultrapassando o conteúdo declarativo do direito ao silêncio.

Por essa razão, entendemos que o privilégio contra a autoincriminação apenas vigora dentro do âmbito do direito ao silêncio, ou seja, o direito a não responder a perguntas.

Apenas o que tem uma natureza declarativa está abrangido pelo artigo 61.º, n.º 1, alínea d) do CPP.

Significa, portanto, que se o que for pedido ao arguido tiver um significado verbal ou comunicacional de que este é culpado este tem o direito a recusar-se a participar.

Se aquilo que for pedido ao arguido for uma informação, como é o caso da palavra passe, então, o fornecimento dessa mesma informação corresponde a uma declaração e, por essa razão, podemos considerar que ele tem o direito a não responder e, em consequência, a não fornecer essa informação.

O privilégio contra a autoincriminação não é absoluto e irrestringível.

[210] *Vide* PINTO DE ALBUQUERQUE – *Comentário*, p. 56, "Nem o arguido, nem o demandado que seja constituído como arguido têm o dever de colaboração com o tribunal ou o MP com vista à "descoberta da verdade material e à boa decisão da causa" (*nemo tenetur se ipsum accusare*), dado o seu direito constitucional ao silêncio (artigo 32.º, n.º 1 da CRP)".

Devem ter-se em consideração dois elementos, por um lado, a tutela efetiva da justiça e o dever de eficácia da investigação e, por outro lado, as garantias de defesa do arguido.[211]

O princípio da proporcionalidade, presente no n.º 2 do artigo 18.º da CRP tem um papel fundamental de fiscalização e de controlo quanto à gestão equilibrada dos elementos em causa, o que significa que o direito à não autoincriminação não pode ser irrestringível, podendo, por isso, ser alvo de algumas limitações quando tal se justifique.

Posto isto, dúvidas não existem quanto à possibilidade de restrição do privilégio contra a autoincriminação "em prol de outros interesses salvaguardados pelo ordenamento jurídico"[212], mas "tal só pode suceder quando existe um comando legal expresso e se encontrarem respeitados os limites constitucionais para a restrição dos direitos fundamentais"[213].

Não pode existir "um total e ilimitado sacrifício da prova a todas as necessidades reais ou presumidas, de processamento e de punição"[214].

Estamos perante uma questão de concordância prática entre, por um lado, as necessidades de apuramento da existência e, eventualmente de punição, de uma determinada conduta e, por outro lado, a reserva da intimidade da vida privada e o direito de defesa.[215]

"E daqui derivam duas consequências: desde logo, a solução da questão tem de obedecer aos cânones do princípio da proporcionalidade em sentido amplo, e por outro, uma incorreta solução cifrar-se-á numa restrição desproporcionada de uma das vertentes em questão, a qual, atendendo aos direitos em questão, bem pode acarretar a nulidade da prova utilizada"[216].

[211] Neste sentido, NEVES, Rita Castanheira; CORREIA, Hélder Santos – "A lei do cibercrime e a colaboração do arguido no acesso aos dados informático". *Actualidad Jurídica.* Madrid: Uría Menéndez. N.º 38 (out. – dez. 2014), p. 146.
[212] *Idem*, p. 147.
[213] *Ibidem*.
[214] LOBO MOUTINHO – *Lei da*, p. 335.
[215] Neste sentido, *idem*, p. 337.
[216] *Ibidem*.

Até 2009, ano da entrada em vigor a LC, não havia qualquer referência quanto à questão do fornecimento de informações respeitantes a suportes informáticos.

A LC veio consagrar, no n.º 5 do artigo 14.º, uma solução especial para estes casos. Estabeleceu, expressamente, a salvaguarda do direito à não autoincriminação, quer quanto ao arguido, quer quanto ao suspeito, o que se traduz numa não obrigatoriedade de revelação de informações pelo arguido ou pelo suspeito.[217]

No caso da apreensão de correio eletrónico, prevista no artigo 17.º da LC, não se consagrou uma "exceção de imposição das medidas processuais ao arguido"[218] como a que se encontra no n.º 5 do artigo 14.º do mesmo diploma.

A não colaboração do arguido não inviabiliza o acesso ao sistema informático, apenas requer que seja proferido um despacho do JIC, caso este entenda que tal diligência se mostre relevante para o processo, e que se proceda, posteriormente, a um desbloqueio técnico do mesmo.[219]

Quanto ao acesso à conta de correio eletrónico, especificamente, quando o arguido não colabora "não há outra forma de aceder a essa conta, a não ser intervindo diretamente junto do servidor/alojador dessa conta"[220].

Importa referir que no caso de o visado não ser o arguido não vigora o direito ao silêncio. Contudo, consideramos que este também não pode ser obrigado a revelar a palavra passe[221], sob pena de a prova ser considerada nula e proibida, nos termos do artigo 126.º, n.º 1 e n.º 3 do CPP[222].

[217] Ao reconhecer-se, expressamente, o direito do arguido a não revelar informação presente no sistema informático, o legislador colocou o arguido fora da possibilidade de ser visado pelo crime de desobediência.
[218] NEVES; CORREIA – *Actualidad*. N.º 38 (out. – dez. 2014), p. 149.
[219] Neste sentido, *ibidem*.
[220] VERDELHO – *Scientia*. T. LVIII. N.º 320 (out.- dez. 2009). p. 742.
[221] No sentido contrário, CONDE CORREIA – *RMP*. Ano 35. N.º 139 (julho-setembro 2014), p. 59.
[222] Aplica-se também no caso de o visado ser arguido.

2.2. Ausência de consentimento do visado

No caso de o visado não colaborar, isto é, não facultar a palavra-passe de acesso ao sistema informático em causa, existe, como referimos *supra*, a possibilidade de a pedir diretamente ao servidor[223].

Podemos então concluir que não é apenas o visado a "pessoa legalmente autorizada"[224] a facilitar o acesso a estes dados.

Esta possibilidade tem como intuito a não inviabilização da investigação, tendo em consideração a importância que a mensagem enquanto meio de prova e a sua apreensão enquanto método de obtenção de prova representam atualmente, com base numa vontade do visado. Se o acesso estivesse, exclusivamente, dependente da vontade do visado, as investigações nas quais fosse imprescindível o acesso às mensagens de correio eletrónico, estariam na verdade, condicionadas e dependentes de uma parte, cujo interesse pode ser conflituante e até contraditório com o próprio objetivo da investigação.

Não podemos, como já referimos *supra*, permitir que as garantias de defesa do arguido, neste caso, do visado, impossibilitem outro princípio fundamental, a boa administração da justiça, a eficácia da investigação criminal.

Porém, embora nos pareça uma solução lógica e simples, este pedido de acesso ao servidor pode "implicar uma cedência de soberania nacional ao permitir que um Estado exerça, no contexto de uma investigação criminal, actos processuais materialmente incidentes sobre o território do outro Estado contactando diretamente a pessoa legalmente

[223] Quanto ao pedido junto do servidor, cfr. TRE – Acórdão de 13 de novembro de 2012, processo n.º 315/11.2PBPTG-A.E1, onde se refere: "Atendendo a que, no presente caso, apenas com o conhecimento dos IPs referentes às comunicações a acessos identificados no decurso da investigação como relevantes para a indiciação dos crimes denunciados se poderá avançar na descoberta da identidade do autor ou autores dos factos em averiguação, entende-se que a obtenção desta informação junto da operadora é indispensável para a descoberta da verdade material, não se vislumbrando outra forma de obter tal prova.
É do nosso conhecimento funcional, por processos de semelhante natureza, que a Google não exige emissão de Carta Rogatória, respondendo as solicitações por email.
Também é do nosso conhecimento funcional que a Google aceita pedidos em português, mas que deve ser feito em papel timbrado do Tribunal, assinado e carimbado pelo JIC, o qual no inicio do texto se deve apresentar quanto a sua qualidade, elencando o crime em investigação, pena em abstracto e a necessidade de obtenção dos elementos para a continuação da investigação no âmbito do processo crime.
Assim, uma vez que a Google não exige a emissão de Carta Rogatória e responde por email, mas apenas mediante despacho de Juiz, promove-se que, através do endereço de correio electrónico … se solicite as seguintes informações…".
[224] RAMALHO – *RDI*. N.º 02 (2014), p. 139.

autorizada a divulgar os dados visados, sem recorrer aos mecanismos de auxílio mútuo"[225].

O recurso a esta possibilidade encontra-se restringido às partes signatárias da Convenção sobre o Cibercrime e não a todos os Estados.

Alguns países, resistentes a esta ingerência na soberania nacional, ainda que membros do Conselho da Europa, recusaram-se a assinar a Convenção sobre o Cibercrime, o que pode levantar alguns problemas na prática.

Numa situação em que o servidor se encontre, por exemplo, na Rússia, embora este país seja membro do Conselho da Europa, o mesmo recusou-se a assinar a Convenção sobre o Cibercrime pelo que os investigadores não terão sucesso no contacto direto com o servidor, para conseguirem aceder à conta.[226]

2.3. Ausência de consentimento da pessoa legalmente autorizada

Situação diferente e um pouco mais complexa acontece quando nem o visado nem a empresa que fornece o serviço, enquanto pessoas legalmente autorizadas a dar acesso ao sistema informático, o concedem para proceder à recolha de prova.

Na adaptação do direito interno à Convenção sobre o Cibercrime, omitiu-se a referência à limitação territorial da apreensão do correio eletrónico, tendo sido feita apenas menção ao acesso a um sistema informático.

Esta realidade pode ser alvo de duas interpretações.

Por um lado, uma interpretação restritiva que determina que, apesar da omissão, a norma deve ser interpretada à luz da Convenção do Cibercrime e, por isso, apenas se aplica em território português, ou seja, só pode ser aplicada quando as mensagens se encontram armazenadas num sistema informático localizado em Portugal. Fora destes casos, as autoridades terão de recorrer aos mecanismos de cooperação internacional.

[225] RAMALHO – *RDI*. N.º 02 (2014), p. 140 e 141.
[226] Cfr. *Idem*, p.141.

Por outro lado, uma interpretação literal e teleológica, que não estabelece qualquer limitação territorial, permitindo o acesso a qualquer sistema informático, independentemente da sua localização, desde que o acesso seja lícito.[227]

Como fundamento para esta última interpretação aponta-se o objetivo de "remover unilateralmente os obstáculos à eficácia da investigação criminal, indo mais longe do que os termos previstos na Convenção"[228].

Esta opção, embora, pareça ser a mais vantajosa para a investigação, pode trazer consequências bastante nefastas para a mesma.

Pensemos num caso em que existem várias investigações, em simultâneo, em diferentes estados, possivelmente pelos mesmos factos, nas quais há a necessidade de se proceder à recolha de prova armazenada no mesmo servidor. Neste caso, o facto de as várias autoridades poderem recolher prova de forma livre pode levar a que a mesma possa ser contaminada, ou inclusivamente, eliminada por uma das entidades que tem contacto com a prova, sem que as outras tenham conhecimento dessa ingerência. Não esquecendo que tal ingerência teria ainda consequências nefastas para os direitos fundamentais do visado. [229]

Cumpre, ainda, referir que, inversamente ao que foi estabelecido para as diligências realizadas pelas autoridades portuguesas em território estrangeiro, o acesso aos sistemas armazenados, em Portugal, por autoridades estrangeiras, para a recolha de prova está vedado, com exceção do previsto no artigo 25.º da LC.[230]

2.4. Conclusões

No decurso de uma investigação, pode mostrar-se necessário e relevante, para a prova, o acesso e a obtenção de mensagens de correio eletrónico.

A ingerência permitida neste tipo de comunicação pode ter como "alvo" não só o arguido, como também qualquer pessoa, desde que esteja verificado o requisito do interesse e relevância. Tem de existir uma ligação mínima entre o processo e a pessoa

[227] Neste sentido, RAMALHO – *RDI*. N.º 02 (2014), p. 143 e VERDELHO – *Scientia*. T. LVIII. N.º 320 (out.-dez. 2009), p. 749.
[228] RAMALHO – *RDI*. N.º 02 (2014), p. 145.
[229] *Idem*. p. 146.
[230] *Idem*, p. 148.

visada pela diligência ou a sua conta de correio eletrónico, mesmo que ela não tenha conhecimento dessa possível ligação.

O destinatário da mensagem passa a ter total legitimidade e disponibilidade sobre a mesma, ainda que não seja ele o seu autor.

O acesso às mensagens de correio eletrónico processa-se de uma forma bastante distinta das cartas tradicionais. O acesso ao correio eletrónico implica o acesso a um sistema informático que só será possível, do ponto de vista técnico, mediante duas situações, com o consentimento do visado ou com uma autorização por parte do servidor que, não tem qualquer correspondência quando está em causa a apreensão de uma carta tradicional, cujo acesso depende apenas da abertura do envelope.

O acesso ao conteúdo do correio eletrónico está, portanto, dependente da vontade de um "terceiro".

Não existindo uma obrigação por parte do visado em fornecer a palavra passe, a investigação corre o risco de ficar, muitas vezes, dependente da autorização do servidor que nem sempre se verifica. O servidor acaba por preferir proteger os dados dos seus clientes, salvaguardando a relação de confiança e segurança que estes sentem em relação à prestação dos seus serviços.

No que diz respeito aos mecanismos de cooperação internacional, embora estejam previstos e regulados na lei, os mesmos nem sempre são, eficazmente, cumpridos na prática.

3. A criação de um regime autónomo no CPP como solução necessária?

A nossa pretensão no presente ponto não passa por sugerir um determinado regime específico ou mesmo criá-lo. Consideramos que tal caberá ao legislador e não nos compete a nós, neste trabalho, substituir-nos a este e criar um articulado, ainda que possamos vir a defender a autonomização do regime, não só quanto à apreensão de correio eletrónico como quanto à prova digital.

O intuito deste ponto é, portanto, o de demonstrar se se justifica ou não o tratamento específico e autonomizado da prova digital, tendo em conta, tudo o que analisámos, anteriormente.

A criação de redes de comunicação eletrónicas, *maxime*, o aparecimento da *Internet*, veio revolucionar a forma como comunicamos, isto é, no fundo, a forma como a informação é transmitida.

O recurso cada vez mais frequente a sistemas informáticos e de comunicação eletrónicos gerou uma nova "realidade", a realidade digital ou virtual.

Se para a própria sociedade, em geral, é difícil acompanhar toda esta evolução que tem ocorrido ao longo dos últimos anos[231], para instituições como Estado, o desfasamento entre a velocidade de evolução desta nova realidade e a velocidade do seu acompanhamento e intervenção de forma atualizada é ainda mais notório.

No Direito e, em particular, no processo penal, o esforço para evitar o aparecimento de espaços vazios e situações de ineficácia ou impunibilidade é constante.

Até há pouco tempo, a prova que entrava para o processo apresentava determinadas características, por exemplo, as perícias e os documentos que, na maioria dos casos, eram perícias médico-legais ou de balística e documentos em suporte físico, respetivamente. Atualmente deparamo-nos com uma nova realidade, a prova digital que inevitavelmente implica a incorporação de novos métodos de obtenção de prova e a adequação dos já

[231] Desde 1991, quando foi criada a Lei da Criminalidade Informática e que corresponde à altura em que o acesso à *Internet*, em Portugal, deixou de ser restrito às redes científicas e universitárias e passou a ser aberto ao público.

existentes a esta nova realidade que, inclusivamente, o próprio avanço tecnológico também permite.

Assistimos, claramente, à mudança de uma realidade paradigmaticamente física e material para uma realidade virtual e imaterial, o que, por si só, já cria algumas necessidades de renovação do sistema jurídico.

"Comprova-se ser necessário esclarecer e dotar as autoridades de novos métodos de investigação, desde que enquadrados pelo acervo constitucional e legal dos direitos à reserva da vida privada, ao sigilo das comunicações e à protecção de dados pessoais, revelando-se, assim, essenciais as ideias de proporcionalidade e de ponderação relativa dos interesses em causa"[232].

"A qualidade da lei vigente é condição essencial para a qualidade do direito. Sem uma boa lei, por melhores que sejam os nossos juristas, dificilmente haverá bom direito"[233].

O progresso científico e tecnológico exige uma constante adaptação e atualização do ponto de vista legislativo. O direito tem de tentar acompanhar, da melhor maneira possível, os avanços da sociedade e munir-se das ferramentas necessárias para conseguir dar resposta aos novos riscos que se geram.

Foram grandes as expetativas quanto à Reforma ao CPP de 2007. No entanto, não se aproveitou o momento para efetuar uma autonomização do direito informático e da prova digital, compilando tudo numa só legislação e terminando com a dispersão de diplomas avulsos que estão em vigor que, por vezes, se mostram contraditórios.

"Defeito repercutido em duas omissões centrais: a) Ausência de um pensamento conceptualmente exigente sobre a tecnologia e semântica dos institutos probatórios em face da evolução tecnológica e da sua repercussão na interação comunicacional e registos de dados b) Inexistência de uma atenção rigorosa às obrigações internacionais do Estado Português"[234].

Em 2009, a LC tentou reagir à rápida evolução que ocorreu entre o início da década de 90, quando foi criada a Lei da Criminalidade Informática, e os primeiros anos do Séc.

[232] ANTUNES – *Ciências policiais*, p. 29.
[233] CONDE CORREIA – *RMP.* Ano 35. N.º 139 (julho-setembro 2014), p. 53.
[234] DÁ MESQUITA – *Processo Penal*, p. 87 e 88.

XXI, revogando, não só, a Lei da Criminalidade Informática, como ainda parte da extensão presente no artigo 189.º do CPP.

Não podemos negar a inovação jurídica motivada pela LC, nomeadamente com a criação de novos institutos processuais e com a introdução de um novo catálogo de crimes presente no seu artigo 11.º que veio alargar o âmbito de aplicação dos meios de obtenção de prova quando está em causa prova em suporte digital.

Porém, em alguns aspetos as expetativas saíram frustradas e noutros gerou-se uma maior desordem e instabilidade legislativa.

"A legitimação dos novos meios de investigação não se faz agora ao ritmo e à medida das novas possibilidades técnicas e como resultado da sua protecção directa sobre o direito… *o que é tecnicamente possível não é, só por si e sem mais, legítimo*"[235].

O regime da apreensão do correio eletrónico apresenta-se como um mecanismo processual fundamental para os processos em que a investigação passa pelo acesso a redes de comunicações eletrónicas.

Atualmente previsto na LC, o regime da apreensão de correio eletrónico foi "apresentado" como um novo regime especial, mas rapidamente se começou a perceber que se limitou a retirar a apreensão das mensagens do âmbito do regime aplicado às escutas telefónicas, colocando-a, por via de uma mera remissão, no âmbito da apreensão de correspondência, traduzindo-se, para muitos, numa equiparação legal do correio eletrónico à correspondência tradicional.

Consideramos, portanto, que ainda não existe uma verdadeira autonomia quanto ao tratamento e recolha da prova digital, nomeadamente quanto à apreensão de mensagens de correio eletrónico.

As características da prova digital exigem que esta tenha um tratamento especial e, por essa razão, a mera aplicação das normas vigentes à realidade digital pode não ser suficiente para resolver e ultrapassar estes novos desafios.

[235] COSTA ANDRADE – *"Bruscamente*, p. 150.

Deve existir uma compilação e autonomização do regime evitando-se a existência de vários regimes avulsos, por vezes divergentes entre si, e que acabam por tratar da mesma maneira realidades diferentes e de maneiras diferentes realidades legalmente semelhantes, através de equiparações e remissões para regimes processuais pensados para uma realidade bem diferente da atual.

A instabilidade legislativa, associada à sua cada vez maior quantidade e complexidade gera, inevitavelmente, a confusão e a desordem, causando aquilo que o direito pretende suprir, a imprevisibilidade e a insegurança jurídicas.

"Parece que depois do esforço de racionalização e sistematização que culminou com a aprovação do Código de Processo Penal de 1987 o legislador escolheu a via regressiva da descodificação sistemática"[236].

No que diz respeito a aspetos estruturantes do processo penal, deve verificar-se uma centralização normativa. Por um lado, importa clarificar qual o regime que deve ser aplicado e facilitar, deste modo, o trabalho do intérprete e do aplicador do direito. Por outro lado, deve "lograr-se um verdadeiro sistema, tendencialmente unitário da prova digital"[237], com um "corpo legislativo integrado, coerente, e uniforme, capaz de satisfazer as necessidades práticas e de salvaguardar o desejável nível ideal de proteção dos direitos individuais"[238].

Poderíamos questionar se poderia ter sentido criar um regime com previsões diferentes para situações diferentes. Tal poderia traduzir-se, por exemplo, na dispensa do conhecimento prévio pelo JIC quando se trate de um processo com um grande volume de mensagens de correio eletrónico, em que o controlo prévio do JIC, que é feito apenas por aquele juiz, pode tornar inviável a produção de prova em tempo útil, assim como a boa prossecução da investigação.

Esta solução embora, à primeira vista, possa parecer facilitadora do processo de produção de prova, traria certamente muitos problemas em matéria constitucional, nomeadamente quanto à questão dos direitos fundamentais e de alguns princípios como o da igualdade, legalidade e validade de prova.

---

[236] CONDE CORREIA – *RMP*. Ano 35. N.º 139 (julho-setembro 2014), p. 54.
[237] *Idem,* p. 56.
[238] *Ibidem.*

Poderíamos questionar, se faria sentido introduzir no processo penal uma perícia digital, isto é, que integre dados digitais. O acesso às mensagens de correio eletrónico pode realizar-se através de uma pesquisa informática ou através de outro acesso legítimo a um sistema informático. Neste caso, poderia ser proveitoso para o sucesso da investigação a previsão de perícias digitais ou informáticas, cujo regime fosse adequado às suas especificidades técnicas.

A prova que se pode obter e a forma como ela pode ser obtida, através da apreensão de correio eletrónico, apresentam características que reforçam a disparidade face a realidades que foram configuradas aquando da criação do CPP. Por essa razão, consideramos que seria profícuo criar um regime autónomo, que esclarecesse algumas das incertezas e dúvidas com que atualmente somos confrontados.

Independentemente do novo regime que deve ser criado, as normas que regulam a obtenção da prova digital devem estar, sempre, em conformidade com o regime geral da obtenção de prova, bem como com os princípios jurídico-constitucionais. Não querendo isto dizer, contudo, que não possam existir algumas exceções e adaptações legalmente previstas, tendo em consideração as especificidades deste tipo de prova e que permitam, da melhor maneira possível, acompanhar o progresso científico e tecnológico.

"O legislador deveria então ter criado um regime autónomo e auto-suficiente, com repartição equilibrada de competências entre o MP e o JIC, a este reservando o estritamente necessário à garantia de direitos dos visados, adequados às suas especificidades técnicas das comunicações electrónicas, muito diferentes da correspondência corpórea, e à estrutura acusatória do processo penal, o que, pelo menos de forma satisfatória não fez no art. 17.º da LCC"[239].

Ainda que se assista cada vez mais a uma realidade jurídica composta por codificações sectoriais, cremos que este novo regime deve integrar-se no CPP, pois só desta forma é que se conseguirá obter um regime uno, claro e em harmonia com o regime geral da prova nele previsto.

[239] CARDOSO – *RMP*. Ano 39. N.º 153 (jan -mar 2018), p. 178, 213 e 214.

Conclusões

A prova é um dos elementos essenciais para a investigação e para o processo penal.

A prova digital apresenta características que criam desafios à atividade probatória, impondo a adequação do atual paradigma de recolha de prova pensado para uma realidade física e material a uma nova realidade digital.

O desenvolvimento dos meios informáticos permitiu o surgimento de novas formas de praticar crimes, novos crimes, bem como uma maior intromissão e ingerência nos direitos dos cidadãos, tendo, ao mesmo tempo, contribuído para novas técnicas de investigação e novos meios de obtenção de prova.

O correio eletrónico surge como uma nova forma de comunicação que merece a proteção constitucional atribuída à correspondência e aos outros meios de comunicação privada.

A sua obtenção encontra-se legalmente legitimada e, por essa razão, não se coloca qualquer questão quanto à sua tipicidade.

Todavia, o atual regime não é suficientemente esclarecido, nem adequado a este meio de comunicação e às circunstâncias em que a sua obtenção se mostra indispensável.

Os vários regimes de obtenção das mensagens de correio eletrónico têm gerado uma incongruência indesejada resultado de uma produção legislativa pouco clara, ambígua e desfasada da realidade, que provoca a desordem, a insegurança e a incerteza jurídicas cujo objetivo do direito é suprir ou menorizar.

A equiparação legal do correio eletrónico à correspondência tradicional é de rejeitar.

De forma inevitável, esta equiparação suscita alguns problemas e mostra-se desajustada face à presente realidade.

Tal reflete-se numa jurisprudência perigosamente contraditória e ameaçadora de um Estado de Direito democrático, onde deve imperar um conjunto de princípios jurídico-constitucionais e de direitos fundamentais cujo núcleo duro não pode ser afetado.

No artigo 17.º da LC não se estabelece qualquer distinção entre mensagens abertas e mensagens fechadas, referindo-se, expressamente, a mensagens armazenadas. Todavia,

em resultado da remissão estalecida no artigo 17.º da LC para o regime do artigo 179.º do CPP não raras são as decisões jurisprudenciais que fazem essa distinção.

Consequentemente, gera-se uma manifesta diminuição da proteção da comunicação. Em resultado de um tratamento diferenciado as mensagens abertas poderão ser livremente apreendidas e o seu conteúdo poderá ser lido por qualquer autoridade que participe na investigação.

Não é o simples facto de se encontrar aberta ou fechada que determina que aquela mensagem deixa de ser comunicação e que o seu conteúdo deixa de merecer a proteção atribuída à mesma.

Esta interpretação provoca uma intromissão e ingerência gravíssimas nas comunicações, afastando, por completo, a proteção das comunicações, bem como o regime de proibição de prova, ambos consagrados na CRP e no CPP.

A ausência de controlo judicial na apreensão e leitura das comunicações é incompatível com o que é constitucional e legalmente estabelecido, atualmente, no nosso ordenamento jurídico.

No regime legal anterior prescindia-se do primeiro controlo judicial na leitura e seleção das mensagens com relevância para a descoberta da verdade e para a prova.

Ainda que tal consubstanciasse uma ingerência nas comunicações, essa ingerência era legalmente admitida, integrando-se, assim, na exceção prevista no artigo 34.º da CRP.

Admite-se que esta solução poderia facilitar e agilizar a investigação, uma vez que não caberia a uma única pessoa, o JIC, a leitura de centenas ou milhares de mensagens quando está em causa, por exemplo, criminalidade altamente organizada ou criminalidade económico-financeira.

Porém, não podemos derrogar o regime estabelecido em 2009 e interpretar a norma segundo os interesses e posições que assumimos no processo e que, inclusive, pode levar a uma contaminação irreparável da prova.

A fragilidade deste meio de prova impõe que a atividade probatória neste âmbito seja realizada com especial cuidado, quer na recolha, quer no tratamento, evitando que sejam

introduzidos, alterados ou até eliminados dados essenciais para a investigação e para o processo.

Importa assegurar que os elementos que são admitidos no processo mantêm o seu valor probatório.

Sob outra perspetiva, levantam-se questões de natureza constitucional relativamente a direitos como a reserva da intimidade da vida privada e o sigilo das comunicações que podem ser severamente afetados, caso não sejam cumpridos os requisitos e os limites estabelecidos pela lei.

Conquanto possa gerar alguns problemas, a norma não deixa margem para dúvidas. Tem de existir uma autorização ou ordem judicial prévia à apreensão e tem de existir um controlo judicial prévio, em primeira linha, quanto ao conteúdo das mensagens que sejam encontradas e possam ser relevantes para a descoberta da verdade e para a prova.

Esta interpretação é a que melhor garante a previsibilidade e a segurança jurídicas, impedindo a derrogação da norma, e a proteção constitucional da mensagem.

O princípio da igualdade e a interpretação e aplicação uniformes da lei, que privilegiem a sua letra e que tenham também em consideração os restantes elementos de interpretação exigem que exista um equilíbrio entre a tutela efetiva da justiça, os direitos fundamentais dos cidadãos e os restantes princípios jurídico-constitucionais.

Deve existir uma ponderação relativa dos interesses em causa com base no princípio da proporcionalidade.

Do ponto de vista técnico, a obtenção deste meio de prova encontra-se dependente da intervenção de terceiros, nomeadamente do consentimento do visado, da autorização do servidor ou, ainda, dos mecanismos de cooperação internacional.

Esta dependência pode limitar o acesso a prova essencial para o decurso de uma investigação quando estes três “elementos” decidem não colaborar.

Este é sem dúvida um dos grandes desafios que o processo penal enfrenta.

Por fim, as sucessivas intervenções legislativas têm-se mostrado, por um lado insuficientes e, por outro lado, causadoras de grandes incongruências no sistema.

Existe, manifestamente, a necessidade de criação de um regime específico, detalhado e autónomo para a apreensão do correio eletrónico que venha clarificar e colmatar alguns dos problemas com que se depara, atualmente, o processo penal.

Bibliografia

ALBUQUERQUE, Paulo Pinto de – *Comentário do Código Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*. 4ª Ed. Atualizada. Lisboa: Universidade Católica, 2011. ISBN 9789725402955.

ANDRADE, José Carlos Vieira de – *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. 5.ª edição. Coimbra: Almedina, 2012. ISBN 9789724046693.

ANDRADE, Manuel da Costa – *"Bruscamente no Verão Passado", a reforma do Código de Processo Penal: observações críticas sobre uma lei que podia e devia ser sido diferente*. Coimbra: Coimbra Editora, 2009. ISBN 9789723217261.

ANTUNES, André Francisco Dias – "Recolha de prova digital – correio electrónico e processo penal: regimes aplicáveis e actuação dos órgãos de polícia criminal". Chambel, Élia Marina; Valente, Manuel Guedes; Santo, Paula do Espírito (Coord.) – *Ciências policiais: Estado, segurança e sociedade.* Coimbra: Almedina, 2011. ISBN 9789724047157.

ANTUNES, Maria João – *Direito Processual Penal.* Coimbra: Almedina, 2016. ISBN 9789724065588.

BRAVO, Rogério – "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta". *Polícia e Justiça*. Coimbra: Coimbra Editora, 2006. ISSN 08704791. N.º7 (jan.jun. 2006) III Série. p. 207-216.

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital — *Constituição da República Portuguesa Anotada: Vol. I.* 4.ª Ed. Revista. Reimpressão. Coimbra: Coimbra Editora, 2006. ISBN 9789723222876.

CARDOSO, Rui – "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX". *Revista do Ministério Público*. ISSN 08706107. Ano 39. N.º 153 (jan -mar 2018). p.167-214.

CASABONA, Carlos Maria Romeo – "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet". *Derecho*

y conocimiento: vol. II. 2006. Huelva. Universidad de Huelva: Facultad de Derecho. ISSN 15788202. p.123-149.

CORREIA, João Conde – "Prova digital: as leis que temos e a lei que devíamos ter". *Revista do Ministério* Público. ISSN 08706107. Ano 35. N.º 139 (julho-setembro 2014). p.29-59.

GABINETE CIBERCRIME – "Nota Prática n.º 6/2015 de 27 de agosto de 2015". Procuradoria Geral da República - *Jurisprudência sobre prova digital*. Acedido a 1 de junho de 2018. Disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_6_jurispridencia_processual.pdf.

GOUVEIA, Jorge Bacelar – *Manual de Direito Constitucional*. Vol. II. 6.ª ed. Coimbra: Almedina, 2016. ISBN 9789724067064.

Machado, João Baptista – *Introdução ao Direito e ao Discurso Legitimador*. 17.ª Reimpressão. Coimbra: Almedina, 2008. ISBN 9789724004716.

MARQUES, José Augusto Garcia; MARTINS, António Gomes Lourenço - *Direito da informática*. 2.ª ed. Coimbra: Coimbra Editora, 2006. ISBN 9724028593.

MENDES, Paulo de Sousa – *Lições De Direito Processual Penal*. Coimbra: Almedina, 2015. ISBN 9789724052052.

MESQUITA, Paulo Dá – *Processo Penal, Prova e Sistema Judiciário*. Coimbra: Wolters Kluver Portugal, 2010. ISBN 9789723218428.

MIRANDA, Jorge; MEDEIROS, Rui – *Constituição Portuguesa Anotada. Tomo I*. Coimbra: Coimbra Editora, 2005. ISBN 9723213987.

MOUTINHO, José Lobo – "Comentário ao Artigo 31.º – Prova". In PORTO, Lopes Manuel; VILAÇA, José da Cruz; CUNHA, Carolina; HENRIQUES, Miguel Gorjão; ANASTÁCIO, Gonçalo (Coord.). HENRIQUES, Miguel, Gorjão (Dir.) – *Lei da Concorrência – Comentário Conimbricense*. Coimbra: Almedina, 2013. ISBN 9789724050607. p. 329-356.

NEVES, Rita Castanheira – *As ingerências nas comunicações eletrónicas em processo penal*. Coimbra: Coimbra Editora, 2011. ISBN 9789723219425.

NEVES, Rita Castanheira; CORREIA, Hélder – "A lei do cibercrime e a colaboração do arguido no acesso aos dados informático". *Actualidad Jurídica*. Madrid: Uría Menéndez. N.º 38 (out. – dez. 2014). p.146-149. Acedido a Disponível em http://www.uria.com/documentos/publicaciones/4377/documento/fp02.pdf?id=5591

PINTO, Ângela – "Crime de abuso sexual de menores com recurso à internet: enquadramento jurídico, prática e gestão processual". Pereira, Luís Silva; Albuquerque, José Ribeiro de; Duarte, Jorge Manuel Vaz Monteiro Dias (Coord.) – *Trabalhos Temáticos de Direito e Processo Penal – Volume I*. Lisboa: Centro de Estudos Judiciários, 2016. Acedido a 1 de junho de 2018. Disponível em http://www.cej.mj.pt/cej/recursos/ebooks/penal/eb_Trabalhos_Tematicos_Direito_Processo_Penal_Vol_I.pdf

PINTO, Frederico de Lacerda da Costa – *A categoria da punibilidade. Vol. II*. Coimbra: Almedina, 2013. ISBN 9789724053790.

RAMALHO, David Silva – "A recolha de prova penal em sistemas de computação em nuvem". *Revista de Direito Intelectual*. N.º 02 (2014). ISBN 9782183258027.

RAMALHO, David Silva – *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017. ISBN 9789724070001.

RODRIGUES, Benjamim Silva – *Direito Penal Parte Especial. Tomo I. Direito Penal Informático-Digital*. Coimbra: Coimbra Editora, 2009. ISBN 9789899577954.

SILVA, Germano Marques da – *Curso de Processo Penal. Vol. II*. Lisboa: Verbo, 2011. ISBN 9789722230438

TONINI, Paolo – "Direito de defesa e prova científica: novas tendências do processo penal italiano". *Revista Brasileira de Ciências Criminais*. ISSN 14155400. Ano 12. N.º 48 (maio-junho 2004). p. 194-214.

VEIGA, Armando; RODRIGUES, Benjamim Silva – *Escutas Telefónicas. Rumo à Monotorização dos Fluxos Informacionais e Comunicações Digitais*. Coimbra: Coimbra Editora, 2007. ISBN 9789892005171.

VERDELHO, Pedro – "A nova Lei do Cibercrime*"*. *Scientia Iuridica*, Braga: Universidade do Minho. ISSN 08709195. T. LVIII. N.º 320 (out.- dez. 2009). p.717-749.

VERDELHO, Pedro – "Apreensão de correio electrónico em Processo Penal". *Revista do Ministério Público*. ISSN 08706107. Ano 25. N.º 100 (outubro/dezembro 2004). p. 153-164.

VERDELHO, Pedro – "A obtenção de prova em ambiente digital". *Revista do Ministério Público*. ISSN 08706107. Ano 25. N.º 99 (julho-setembro 2004). p.117-136.

Jurisprudência

TRIBUNAL DA RELAÇÃO DE COIMBRA – Acórdão de 4 de fevereiro de 2015. Processo n.º 73/14.9JALRA-A.C1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/85a30a1f50f67a2780257de8004fd90b?OpenDocument.

TRIBUNAL DA RELAÇÃO DE COIMBRA – Acórdão de 7 de junho de 2017. Processo n.º 96/14.8EALSB-A.C1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/4a635f3366957e7c8025813a0036956c?OpenDocument.

TRIBUNAL DA RELAÇÃO DE ÉVORA – Acórdão de 13 de novembro de 2012. Processo n.º 315/11.2PBPTG-A.E1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/d147ed8908009d4980257de10056f9c9?OpenDocument.

TRIBUNAL DA RELAÇÃO DE ÉVORA – Acórdão de 6 de janeiro de 2015. Processo n.º 6793/11.2TDLSB-A.E1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument.

TRIBUNAL DA RELAÇÃO DE ÉVORA – Acórdão de 20 de janeiro de 2015. Processo n.º 648/14.6GCFAR-A.E1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument.

TRIBUNAL DA RELAÇÃO DE GUIMARÃES – Acórdão de 12 de outubro de 2009. Processo n.º 1396/08.1PBGMR-A.G1. Acedido a 1 de junho de 2018. Disponível emhttp://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/4c03909839f95d5f8025767e004f83fe?OpenDocument.

TRIBUNAL DA RELAÇÃO DE GUIMARÃES – Acórdão de 29 de março de 2011. Processo n.º 735/10.0GAPTL – A.G1. Acedido a 1 de junho de 2018. Disponível emhttp://www.dgsi.pt/jtrg.nsf/c3fb530030ea1c61802568d9005cd5bb/6aa96edf91e899b2802578a00054631f?OpenDocument.

TRIBUNAL DA RELAÇÃO DE GUIMARÃES – Acórdão de 15 de outubro de 2012. Processo n.º 68/10.1GCBRG.G1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/d7e67584752588c980257aa0004607bc?OpenDocument.

TRIBUNAL DA RELAÇÃO DE LISBOA – Acórdão de 15 de julho de 2008. Processo n.º 3453/2008-5. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrl.nsf/0/9182245992c7c5d18025749000503b8c?OpenDocument.

TRIBUNAL DA RELAÇÃO DE LISBOA – Acórdão de 11 de janeiro de 2011, processo n.º 5412/08.9TDLSB-A.L1-5. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrl1.nsf/0/e5ed1936deb44eb180257824004ab09d?OpenDocument.

TRIBUNAL DA RELAÇÃO DE LISBOA – Acórdão de 2 de março de 2011. Processo n.º 463/07.3TAALM-A.L1-3. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d10c400a16882e9e80257853005d65c1?OpenDocument.

TRIBUNAL DA RELAÇÃO DE LISBOA – Acórdão de 20 de dezembro de 2011. Processo n.º 36/11.6PJOER-A.L1-5. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/f1248a82449c5ffd8025798200445cb2?OpenDocument.

TRIBUNAL DA RELAÇÃO DE LISBOA – Acórdão de 29 de março de 2012. Processo n.º 744/09-1S5LSB-A.L1-9. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/3fadd3f921c9d6588025 79e2004500c9?OpenDocument.

TRIBUNAL DA RELAÇÃO DE LISBOA – Acórdão de 24 de setembro de 2013, processo n.º 145/10.9GEALM.L2-5. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c60dfe830c97cf8980257c0000368afa?OpenDocument.

TRIBUNAL DA RELAÇÃO DE LISBOA – Acórdão de 6 de fevereiro de 2018, processo n.º 1950/17.0 T9LSB-A.L1-5. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument.

TRIBUNAL DA RELAÇÃO DO PORTO – Acórdão de 27 de janeiro de 2010. Processo n.º 896/07.5JAPRT.P1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/68fdcdf35dc62b6e802576c40041c799.

TRIBUNAL DA RELAÇÃO DO PORTO – Acórdão de 12 de setembro de 2012. Processo n.º 787/11.5PWPRT.P1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/877e0322acde18d080257a8300393cc6?OpenDocument.

TRIBUNAL DA RELAÇÃO DO PORTO – Acórdão de 3 de abril de 2013. Processo n.º 856/11.1PASJM.P1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d21c6752627b971780257b4f003caa5d?OpenDocument.

TRIBUNAL DA RELAÇÃO DO PORTO – Acórdão de 24 de abril de 2013, processo n.º 585/11.6PAOVR.P1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/872f3063233d8de480257b78003e60f3?OpenDocument.

TRIBUNAL DA RELAÇÃO DO PORTO – Acórdão de 22 de maio de 2013, processo n.º 74/07.3PASTS.P1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/abf6a7fedb6f7ba580257b88004ed413?OpenDocument.

TRIBUNAL DA RELAÇÃO DO PORTO – Acórdão de 13 de abril de 2016. Processo n.º 471/15.0T9AGD-A.P1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument.

TRIBUNAL DA RELAÇÃO DO PORTO – Acórdão de 21 de fevereiro de 2018. processo n.º 17448/17.4T8PRT.P1. Acedido a 1 de junho de 2018. Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/db6c51e0b5d7e725802582500053165c?OpenDocument.

Índice