UNIVERSIDADE
CATÓLICA
PORTUGUESA

Faculdade de Direito - Escola de Lisboa

Mestrado Forense

O CORREIO ELETRÓNICO COMO MEIO DE PROVA EM PROCESSO PENAL

Dissertação de Mestrado orientada pelo

Senhor Professor Doutor Germano Marques da Silva

Rita Maria Coelho Salvado Pratas

Agosto de 2018

AGRADECIMENTOS

À Faculdade de Direito da Universidade Católica de Lisboa, por todos os ensinamentos que me proporcionou e que levarei comigo pela vida fora.

Ao Senhor Professor Doutor Germano Marques da Silva, pela sua constante disponibilidade, simpatia e conselhos sábios que me foi dando ao longo desta jornada.

Ao Gonçalo pela enorme paciência que sempre teve, pelo apoio incondicional e estimulo que me deu para continuar.

Aos meus pais e à minha avó, por todo o sacrifício e apoio que me deram, mesmo nos gestos mais simples.

Ao meu avô, a minha fonte de inspiração que, mesmo longe, continua e continuará sempre a fazer parte de todos os momentos da minha vida.

ÍNDICE

Página

1. Introdução 6

2. O correio eletrónico enquanto meio comunicacional ……..……7

3. Legislação sobre a prova digital 9

3.1. Legislação no plano internacional..... 9

3.1.1. A Convenção sobre o Cibercrime, de 23 de Novembro de 2001 ..... **10**

3.1.2. A Decisão Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005 ..... **11**

3.1.3. A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006 ..... **11**

3.2. Legislação no plano nacional 13

3.2.1. O artigo 189º do Código de Processo Penal..... **13**

3.2.1.1. Da (in)adequação da cláusula de extensão do art. 189º do CPP.....**14**

3.2.1.2. Da extensão do art. 189º do CPP às mensagens de correio eletrónico (ou equiparáveis) "*que se encontrem guardadas em suporte digital*". A interceção do correio eletrónico em tempo real e a subsunção ao regime das buscas ... **15**

3.2.1.3. Da ingerência em tempo real do correio eletrónico (e equiparáveis): a necessidade de uma autonomização do regime **19**

3.2.1.4. Da "*interceção das comunicações entre presentes*"..... **21**

3.2.2. A Lei da Conservação de Dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas (Lei n.º 32/2008, de 17 de julho) **23**

3.2.3. Da Lei da Cibercriminalidade Informática (Lei n.º 109/91) à atual Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro)..... **25**

4. O correio eletrónico: Confronto entre os vários diplomas 32

4.1. A Lei n.º 32/2008 e a Lei n.º 109/2009 32

4.2. A Lei n.º 109/2009 e o Código de Processo Penal 33

4.2.1. O regime jurídico aplicável à ingerência nas comunicações armazenadas em suporte digital: críticas **34**

4.2.2. O regime da interceção e registo de comunicações eletrónicas em tempo real..... ..... **37**

4.3. A Lei n.º32/2008 e o art. 189º do CPP 39

5. A utilização do correio eletrónico: considerações acerca das implicações jurídico-constitucionais 40

5.1. Os direitos implicados 40

5.1.1. O art. 34º da CRP **40**

5.1.2. O art. 35º da CRP **43**

5.1.3. O art. 26º da CRP **43**

6. Algumas reflexões sobre a prova digital e o correio eletrónico - Perspetivas de futuro 47

6.1. As especificidades da prova digital 47

6.2. Dificuldades suscitadas pela sua natureza 48

6.3. Perspetivas de futuro: propostas a considerar 49

7. Considerações Finais 52

8. Referências Bibliográficas 55

Jurisprudência Citada **59**

Legislação Consultada **60**

SIGLAS E ABREVIATURAS

Ac. – Acórdão

APUD - citado por

Art.- artigo

Cf.- confira

CPP- Código do Processo Penal

CRP- Constituição da República Portuguesa

JIC- Juíz de Instrução Criminal

MP- Ministério Público

Op. cit. – obra citada

OPC- Órgãos de Policia Criminal

pp. - páginas

ss.- seguintes

TIC- Tecnologias da Informação e da Comunicação

TJUE- Tribunal de Justiça da União Europeia

Vg.- veja-se

1. INTRODUÇÃO.

A presente dissertação tem como objetivo apresentar uma reflexão crítica sobre a natureza e regime jurídico do correio eletrónico enquanto meio de obtenção de prova em processo penal.

Para tal, começamos por uma primeira aproximação ao conceito de correio eletrónico, tema central do nosso estudo.

De seguida, analisamos a legislação internacional sobre o tema, dando relevo à Convenção sobre o Cibercrime, de 23 de Novembro de 2001; à Decisão Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005 e à Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006.

Posteriormente, realçamos as respostas legislativas dadas pelo ordenamento jurídico português, focando, em especial, o que se refere à obtenção de prova digital, e a relevância da Lei n.º 32/2008, de 17 de Julho e da Lei n.º 109/2009, de 15 de Setembro.

Dada a importância do Código de Processo Penal (doravante CPP), é nosso intuito debruçar-nos sobre a forma como este se harmoniza ou conflitua com os diplomas atrás referidos. No conjunto das questões analisadas, ressalta a ideia de que, em virtude das disparidades na regulamentação destes diplomas, muitas são as questões em aberto sobre as quais a doutrina se tem vindo a debruçar.

Indelevelmente ligados ao regime do correio eletrónico apresentam-se os desígnios constitucionais como *a privacidade, a palavra, a salvaguarda da inviolabilidade das comunicações e a autodeterminação informacional*, questões que têm vindo a sofrer algum desgaste fruto dos recentes progressos tecnológicos e que, por isso, merecem ser aqui objeto de reflexão.

Por fim, cientes que existem várias dificuldades suscitadas pela natureza da prova digital, designadamente a dificuldade da sua recolha e conservação, e a possibilidade desta ser facilmente manipulável, procurámos apresentar novas perspetivas, não com a pretensão de chegar a uma solução inequívoca, mas, pelo menos, com a ambição de procurar uma resposta mais adequada para a problemática.

2. O CORREIO ELETRÓNICO ENQUANTO MEIO COMUNICACIONAL

Nas últimas décadas, com o advento das novas tecnologias, impulsionadas pelo surgimento da Internet, as formas de comunicação mudaram substancialmente.

Se antes a única forma de fazer chegar uma mensagem até um destinatário longínquo era através de fax ou carta, hoje a comunicação assenta "em meios técnicos, as redes ou sistemas de telecomunicações - fios, cabos ou outras coisas de natureza corpórea, e espetro radioelétrico, satélites -, meios que contribuem para que a distância que separa uns homens dos outros deixe de constituir um obstáculo à troca recíproca de informações e, portanto, à comunicação entre eles."[1]

Neste contexto ocupa lugar cimeiro o correio eletrónico que, constituindo um meio de comunicação mais expedito e menos dispendioso "veio revolucionar a forma como comunicamos."[2]

Na alínea h) do art. 2º da Diretiva nº 2002/58/CE do Parlamento e do Conselho, de doze de julho de dois mil e dois (relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas), o legislador europeu definiu *correio eletrónico* como "qualquer mensagem textual, vocal, sonora ou gráfica enviada através da rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário as recolher".

A abrangência e caráter vago desta definição de correio eletrónico cria uma "zona cinzenta" que deixa, assim, espaço para várias outras tentativas de definição.

Segundo Romeo Casabona, por exemplo, o correio eletrónico é "uma modalidade de comunicação, em geral de caráter pessoal, que incorpora texto, som ou imagem e que utiliza as redes telemáticas como tecnologia de transmissão e os sistemas informáticos (computadores e o software ou sistema lógico correspondente) como instrumentos de emissão e receção entre dois ou mais comunicantes e, nesse caso, de armazenamento de mensagens"[3] (tradução nossa).

---

[1] GONÇALVES, Pedro Costa - *Direito das Telecomunicações*, 1999, p. 9
[2] RAMOS, Armando Dias - *A prova digital em Processo Penal: o correio eletrónico*, 2014, p.21
[3] ROMEO CASABONA, Carlos Maria - La protección penal de los mensajes de correo eletrónico y de otras comunicaciones de caráter personal a través de internet", 2004, p. 129

Armando Veiga e Benjamim Silva Rodrigues, por sua vez, definem *correio eletrónico* como "um fluxo informacional e comunicacional digital, sob o formato de texto, voz, som, informacional e comunicacional (tendencialmente) fechado, através de um ponto terminal da rede, na rede pública de comunicações eletrónicas, conduzida até ao servidor de mail ou ao terminal do destinatário de fluxo até que o mesmo proceda à sua recolha, leitura e/ou posterior eliminação."[4]

Com a Lei n.º 48/2007, de vinte e oito de agosto, que procedeu à 15.º alteração ao Código de Processo Penal, persistiu a opção do legislador por uma formulação ambígua de correio eletrónico, deixando em aberto muitas questões.

Tal facto levou a que, equivocamente, grande parte da doutrina e jurisprudência portuguesa se inclinasse para uma equiparação legal do correio eletrónico com a tradicional correspondência em papel, questão sobre a qual nos debruçaremos em momento posterior[5].

[4] VEIGA, Armando e RODRIGUES, Benjamim Silva - *Escutas Telefónicas. Rumo à Monitorização dos Fluxos Informacionais e Comunicacionais Digitais*, 2007, p. 374
[5] A este respeito, *vg*. pp. 33-35 do presente trabalho

3. LEGISLAÇÃO SOBRE A PROVA DIGITAL

A legislação sobre prova digital encontra-se dispersa por vários diplomas, o que conduziu a "incoerências das soluções legais e, sobretudo, ao seu indesejável e nefasto insucesso prático."[6]

Também a existência de legislação internacional sobre esta matéria e o seu necessário processo de transposição para a legislação nacional pelos Estados-Membros, densificaram ainda mais as assimetrias e incoerências existentes.

Dada a relevância da questão, ao longo do presente capítulo procuraremos relacionar a legislação internacional e a nacional em matéria de prova digital.

3.1. LEGISLAÇÃO NO PLANO INTERNACIONAL

A cibercriminalidade é, cada vez mais, uma realidade transfronteiriça. Benjamim Silva Rodrigues afirma a este propósito que ocorreu "uma mutação qualitativa e quantitativa no "palco da guerra". Os actores deixaram de ser os Estados, para passarem a ser os grupos criminosos organizados, globalizados e transnacionais. A guerra tradicional deu lugar à "ciberguerra" e ao "ciberterrorismo"."[7]

Neste novo contexto internacional e perante a necessidade de travar a ascensão de uma criminalidade global e transnacional, a resposta dos Estados-Membros da União Europeia surge de forma concertada e como resultado de cooperação entre os envolvidos. Evidência de tal facto são os vários diplomas internacionais produzidos no âmbito da criminalidade informática e, em particular, no que se refere à prova digital.

De entre a extensa regulamentação internacional, destacamos três diplomas que, no âmbito da prova digital, produziram um forte impacto na legislação portuguesa: a Convenção sobre o Cibercrime, de vinte e três de novembro de dois mil e um; a Decisão Quadro 2005/222/JAI do Conselho, de vinte e quatro de fevereiro de dois mil e cinco e a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de quinze de março de dois mil e seis.

---

[6] CORREIA, João Conde - Prova Digital: as leis que temos e a lei que devíamos ter, 2014, p. 139

[7] RODRIGUES, Benjamim da Silva - *Das escutas telefónicas - A monitorização dos fluxos informacionais e comunicacionais*, Tomo I, 2008, p. 50

3.1.1. A Convenção sobre o Cibercrime, de 23 de Novembro de 2001

No quadro do Conselho da Europa foi aprovada em Budapeste, no dia vinte e três de novembro de dois mil e um, a Convenção sobre o Cibercrime, também designada por "Convenção sobre a Cibercriminalidade".

Considerada "o primeiro e mais importante trabalho internacional de fundo sobre crime no ciberespaço"[8], a Convenção sobre o Cibercrime teve como principal objetivo a criação de mecanismos de proteção da "sociedade contra a criminalidade no ciberespaço, designadamente através da adoção de legislação adequada e da melhoria da cooperação internacional."[9]

Em termos mais específicos, e como sintetiza Renato Lopes Militão[10], a Convenção sobre o Cibercrime procurou "harmonizar as legislações nacionais, fundamentalmente no que concerne à: - delimitação de conceitos jurídico-informáticos; - tipificação de *cibercrimes*; - fixação de regras sobre a aplicação espacial da lei penal relativamente a estes crimes; - consagração de medidas processuais de obtenção de *prova digital*; - implementação de medidas de cooperação internacional com o mesmo objetivo e, genericamente, de *combate à criminalidade informática*."

Portugal subscreveu a Convenção sobre o Cibercrime no ano de dois mil e um, mas o diploma só viria a entrar em vigor no ano de dois mil e nove, aprovado pelo Decreto do Presidente da República nº 92/2009[11], publicado no Diário da República, Série I, de dezasseis de abril e pela Resolução da Assembleia da República n.º 88/2009[12], publicada no Diário da República, Série I, de dia quinze de setembro.

É na sequência da ratificação portuguesa à Convenção sobre o Cibercrime e da necessidade de transposição deste diploma para o ordem jurídica interna, que entra em vigor a Lei n.º 109/2009 (vulgarmente conhecida como Lei do Cibercrime) e que foi transposta a Decisão-Quadro n.º 2005/222/JAI do Conselho, de vinte e quatro de fevereiro relativa a ataques contra sistemas de informação[13].

---

[8] Proposta de Lei n.º 289/X/4.ª – Lei do Cibercrime - Exposição dos motivos
[9] Preâmbulo da Convenção sobre o Cibercrime
[10] MILITÃO, Renato Lopes - A Propósito da Prova digital, 2012, p. 271
[11] Consultado em https://dre.pt/web/guest/pesquisa/-/search/603879/details/normal?q=Decreto-Lei+do+Presidente+da+Rep%C3%BAblica+92%2F2009
[12] Consultado em https://dre.pt/web/guest/pesquisa/-/search/489698/details/maximized
[13] A este respeito, vg. 3.1.2 e 3.2.3 neste trabalho

3.1.2. A Decisão Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005

Tal como a Convenção sobre o Cibercrime, a Decisão-Quadro 2005/222/JAI do Conselho teve por objetivo a harmonização legislativa entre os Estados-Membro da União Europeia, promovendo o reforço da "cooperação entre as autoridades judiciárias e outras autoridades competentes […] mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação"[14]. Adverte, ainda, que a "natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio."[15]

3.1.3. A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006

A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de quinze de março de dois mil e seis, que alterou a Diretiva 2002/58/CE, teve como principal objetivo a harmonização das disposições dos Estados-Membros relativas à "conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações"[16], de forma a "garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves, tal como definidos no direito interno de cada Estado-Membro"[17]. Ou seja, "o objetivo material desta diretiva é, pois, contribuir para a luta contra a criminalidade grave e, assim, em última análise, para a segurança pública."[18]

A Diretiva 2006/24/CE viria a ser transposta para o ordenamento jurídico português através da Lei n.º 32/2008, de dezassete de julho. Contudo, oito anos após a entrada em vigor da referida Diretiva, esta foi declarada inválida pelo Acórdão do Tribunal de Justiça da União Europeia, de oito de abril de dois mil e catorze.

---

[14] Ponto (1) da Decisão Quadro n.º 2005/222/JAI do Conselho, de 24 de Fevereiro
[15] *Ibid.,* Ponto (5)
[16] MILITÃO, *op. cit*., p. 272
[17] Art. 1º, nº1 da Diretiva 2006/24/CE
[18] Ponto 41 do Acórdão do TJUE, de 8 de Abril de 2014. Proc. n.º C-293/12

De entre a extensa fundamentação invocada pelo Tribunal de Justiça da União Europeia (doravante TJUE) para sustentar a invalidade da Diretiva, sublinhamos o argumento de que esta seria aplicada indistintamente a todas as pessoas, não tendo sido levado em conta o princípio da proibição de excesso.

Além de não estabelecer critérios objetivos que permitissem delimitar o acesso das autoridades nacionais competentes aos dados sensíveis[19], "a Diretiva 2006/24 não estabelece critérios objetivos que permitam limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário à luz do objetivo prosseguido"[20]. No que respeita à duração da conservação dos dados, a Diretiva 2006/14/CE não especifica "a determinação do período de conservação"[21], apenas delimita o período de um mínimo de seis meses a um máximo de vinte e quatro meses.

Atente ao atrás exposto, conclui o TJUE, no ponto 65 do referido Acórdão, que, uma vez que a Diretiva "não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta, impõe-se, pois, concluir que esta diretiva comporta uma ingerência nestes direitos fundamentais, de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário."

A decisão do TJUE de invalidar a Diretiva não prejudicou, contudo, a vigência da Lei n.º 32/2008. Apesar deste diploma legal resultar da transposição da Diretiva 2006/24/CE (atualmente revogada), importa ter presente que a validade de atos nacionais só pode ser apreciada pela Assembleia da República. Assim, apesar da "lei mãe"- Diretiva 2006/24/CE- ter sido invalidada, a Lei n.º 32/2008 mantem-se em vigor no ordenamento jurídico português[22].

[19] *Ibid.*, Pontos 59 e 60
[20] *Ibid.,* Ponto 62
[21] *Ibid.*, Ponto 64
[22] Apesar de reconhecermos a importância desta questão, optamos por não a desenvolver, de forma a não extravasar o âmbito da presente dissertação. Sublinhamos apenas o facto de que em países como a Bulgária, Roménia, Alemanha, Chipre e República Checa, a desarmonia entre o regime previsto nesta Diretiva e as constituições nacionais deu origem a declarações de inconstitucionalidade das normas resultantes da transposição da referida Diretiva (a este respeito *vg.* OLIVEIRA, Margarida Viana Guarda de - *Proteção de Dados Pessoais nas Comunicações Eletrónicas*, 2015, p. 34)

3.2. LEGISLAÇÃO NO PLANO NACIONAL

Em Portugal, a prova digital, além de ser regulada no artigo 189º do CPP, encontra-se também prevista na Lei n.º 32/2008, de dezassete de julho (relativamente à conservação de dados gerados ou tratados no âmbito da oferta que temos pelos serviços de comunicações eletrónicas) e na Lei n.º 109/2009, de quinze de setembro (Lei do Cibercrime).

3.2.1. O artigo 189º do Código de Processo Penal

Tendo por base o Decreto-Lei n.º 78/87, de dezassete de fevereiro, o atual CPP sofreu, ao longo dos tempos, sucessivas alterações legislativas.

Na versão originária do CPP, de mil novecentos e oitenta e sete, a extensão do regime das escutas telefónicas estava consagrada no art. 190º e estendia o regime dos artigos 187º a 189º às "*conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone*". Ou seja, o regime das escutas telefónicas no processo penal era aplicado a todos os meios técnicos que fossem "diferentes do telefone".

Com o avanço das tecnologias da informação e da comunicação que, como refere Vera Marques Dias, "tentacularmente se conseguiram infiltrar em todos os ramos da nossa vida"[23] levando ao aprimoramento da atividade criminosa, impunha-se a alteração do preceito em vigor.

A reforma do CPP, em dois mil e sete, introduziu alterações significativas, entre elas, a inversão na ordem dos artigos 189º e 190º do CPP, passando, desta forma, o art. 189º a estatuir a cláusula de extensão do regime das escutas telefónicas, e o art. 190º o efeito de nulidade.

A reforma do CPP operada em dois mil e sete consagrou no n.º1 do artigo 189º a extensão do regime das escutas à interceção das comunicações entre presentes, acrescentou uma significativa menção quanto à interceção do correio eletrónico ou outras formas de transmissão de dados por via telemática "*mesmo que se encontrem guardadas em suporte digital*" e passou a consagrar, no n.º2, a extensão do regime das escutas também à localização celular e dados de tráfego.

[23] DIAS, Vera Elisa Marques - A problemática da investigação do Cibercrime, 2012, p. 65

Contudo, várias têm sido as vozes discordantes que alertam para as incongruências suscitadas pelos aditamentos do art. 189º do CPP. É sobre estas dificuldades que subsistem no regime legal em vigor que irão incidir as reflexões que se seguem.

3.2.2.1. Da (in)adequação da cláusula de extensão do art. 189º do CPP

Preocupado em responder de forma adequada aos novos desafios trazidos pelos progressos cientifico-tecnológicos, o legislador decidiu estender o regime das escutas telefónicas a outros meios de comunicação eletrónica emergentes.

Assim, na reforma do CPP, de mil novecentos e noventa e oito, o legislador estendeu o regime jurídico já existente para as escutas telefónicas "*às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática*", nos termos do então art.190º do CPP.

Com esta redação, o legislador veio dissipar algumas dúvidas que subsistiam na doutrina, uma vez que, até aqui, a doutrina maioritária entendia que o regime das escutas telefónicas se aplicava a outros meios de comunicação que transmitissem uma mensagem.

No atual art. 189º do CPP é dito de forma perentória que o regime das escutas telefónicas se estende a todos os tipos de telecomunicações.

Com este preceito, o legislador pretendeu equiparar o regime das escutas telefónicas enquanto meio de obtenção de prova em processo penal, a todas as demais telecomunicações, com particular destaque para o correio eletrónico.

Todavia, apesar de em ambos os casos estarmos perante uma telecomunicação, a diversidade de natureza do telefone e do correio eletrónico fez com que a extensão operada no art. 189º do CPP fosse alvo de severas críticas.

No que concerne a este ponto, note-se a apreciação de Rita Castanheira Neves[24] que distingue entre a palavra falada e escrita, com base na proteção legal conferida a uma e outra. Segundo esta autora, a diferença entre ambas assenta na "volatilidade da palavra falada. Numa conversação telefónica, a palavra é dirigida para se extinguir naquele mesmo tempo e propósito. Não é suposto haver qualquer tipo de perpetuação do que vai

[24] NEVES, Rita Castanheira - *As ingerências nas Comunicações Eletrónicas em Processo Penal*, 2011

dito. Ao contrário, quando se escreve, sabe-se que se eterniza uma mensagem, seja privada ou não."[25]

Neste sentido, José de Faria Costa defende que devia entender-se da leitura da remissão para as comunicações efetuadas por qualquer meio técnico diferente do telefone, constante do art. 189º do CPP, que nela só podiam contemplar-se os "novos meios de telecomunicação da palavra falada."[26]

Também Benjamim da Silva Rodrigues[27] entende que não deviam ter sido incluídas as ingerências em comunicações eletrónicas escritas no regime jurídico das escutas telefónicas, uma vez que a proteção a conferir às intromissões em fluxos informacionais e comunicacionais provenientes de comunicações faladas e escritas deve ser distinto[28].

Concordamos com esta argumentação, uma vez que não podemos reconduzir realidades diametralmente opostas ao mesmo regime. Com o aparecimento da "palavra virtual"[29] impunha-se ao legislador uma alteração da legislação processual penal em matéria de escutas telefónicas, de forma a acompanhar os novos meios tecnológicos. Apesar das inovações trazidas em matéria de prova digital pela reforma do CPP, em dois mil e sete, consideramos que o legislador português, ao tentar adaptar o regime das escutas telefónicas a outros meios de comunicação, ficou aquém das espectativas. Para além disso, ao misturar realidades distintas, acabou por gerar mais interrogações.

3.2.2.2. Da extensão do art. 189º do CPP às mensagens de correio eletrónico (ou equiparáveis) "*que se encontrem guardadas em suporte digital*". A interceção do correio eletrónico em tempo real e a subsunção ao regime das buscas

A segunda parte do n.º 1 do art. 189º do CPP consagra a extensão do regime das escutas telefónicas às mensagens de correio eletrónico (ou equiparáveis) "*que se encontrem guardadas em suporte digital*".

[25] *Ibid*., p.173
[26] COSTA, José Francisco de Faria - *Direito Penal da Comunicação: alguns escritos*, 1998, pp. 174-175
[27] RODRIGUES, Benjamim da Silva - *Das escutas telefónicas*, Tomo I, 2008
[28] *Ibid*., p.60
[29] Cf. COSTA, *op. cit*., p. 151-152

Para Pedro Verdelho[30] importa diferenciar as mensagens de correio eletrónico recebidas que não foram lidas, e as que já foram lidas. Assim, se, por um lado, as primeiras são correspondência e, por isso, devem ser submetidas ao regime da apreensão da correspondência (art. 179º do CPP), por outro, as segundas são "meros documentos guardados no computador"[31] e, por isso, só podem ser apreendidas no decurso de uma busca.

Não partilhamos do mesmo entendimento. A nosso ver, esta nova menção do art. 189º do CPP, trazida pela reforma do CPP, de dois mil e sete, não faz qualquer sentido, uma vez que não podemos aplicar o mesmo regime que regula as intromissões nas telecomunicações, a algo que (já) não é uma comunicação.

Intercetar uma telecomunicação significa interferir no curso de algo que se encontra em circulação. Assim, entendemos que só pode haver interceção do correio eletrónico em tempo real enquanto este estiver a circular pelas redes[32].

Após o destinatário ler o correio eletrónico, este já cumpriu a sua função e, por isso, já não podemos afirmar que continuamos a estar perante uma comunicação eletrónica. Nesta fase, o correio eletrónico é apenas um "documento" ou ficheiro armazenado no computador ou na conta de e-mail do destinatário e, por isso não pode ser intercetado[33].

Nesta linha de pensamento, Rita Castanheira Neves[34] e Manuel da Costa Andrade[35] defendem que as mensagens de correio eletrónico (e equiparáveis) que se encontrem guardadas em suporte digital, não podem ser subsumidas ao regime das escutas telefónicas, mas sim ao regime das buscas e apreensões.

---

[30] VERDELHO, Pedro - Apreensão do correio eletrónico em processo penal, 2004b
[31] *Ibid.,* p. 158
[32] A este respeito *vg.* MARQUES, Garcia e MARTINS, Lourenço - *Direito da Informática*. 2006. Nesta obra, os autores descrevem minuciosamente o percurso realizado pelo correio eletrónico na rede, até chegar ao seu destinatário, referindo que um e-mail se inscreve "no quadro da correspondência privada, na medida em que há lugar a uma transferência de dados pessoais, sendo consideráveis os riscos de ocorrência de desvios, antes do mais ao redor do endereço eletrónico (endereço IP). Uma mensagem escrita em linguagem corrente, sem criptografia, pode ser lida por numerosos intermediários, se assim o desejarem. O correio eletrónico utiliza um caminho tecnicamente complexo antes de atingir o seu destinatário, uma vez que circula na rede efetuando "saltos" de servidor em servidor. Pode, portanto, ser facilmente intercetado por numerosos leitores […] Existe, pois, uma potencialidade efetiva de espionagem dos endereços que assim circulam na rede." *Ibid.*, pp. 433-434
[33] CARDOSO, Vanessa Chagas - *Telecomunicações e prova em processo penal: das escutas telefónicas à intromissão nas comunicações eletrónicas*, 2014, p. 37
[34] NEVES, o*p. cit.*, pp. 182-183
[35] ANDRADE, Manuel da Costa – *Bruscamente no Verão Passado (...)*, 2009, p. 185

Manuel da Costa Andrade vai mais longe, apelidando o art. 189º do CPP de "casa dos horrores hermenêuticos"[36]. Segundo este autor, ao englobar "várias realidades distintas, necessitadas de tutela e exigências distintas, causando incerteza e insegurança jurídicas"[37], este artigo vem trazer novas dificuldades às instâncias formais de controlo.

Partilhamos desta visão, uma vez que, ao subsumir o correio eletrónico guardado no computador ao regime de escutas telefónicas, o legislador põe em causa a investigação criminal. Mais, entendemos que o art. 189º do CPP coloca entraves significativos na atuação do Ministério Público (doravante MP), dos Órgãos de Policia Criminal (doravante OPC), uma vez que, como bem sintetiza o Acórdão do Tribunal da Relação de Coimbra, de 28-01-2009, "sempre que for apreendido um computador, o MP deve fazer intervir o juiz de instrução antes de investigar o conteúdo do computador, pois é previsível que ele contenha comunicações eletrónicas mesmo que já tenham sido lidas. Autorizado judicialmente o acesso ao computador, o OPC acede ao conteúdo do mesmo, toma conhecimento do teor do correio eletrónico e no prazo assinalado no artigo 188º, n.º 3 leva-o ao conhecimento do MP, com os suportes técnicos e os autos e relatórios referidos no n.º1 do dito artigo. Seguidamente o MP apresenta esses elementos ao juiz de instrução, dentro de 48 horas, nos termos e para os efeitos do artigo 188º n.º 4."[38]

Atente ao exposto, entendemos estar perante um obstáculo na investigação criminal, uma vez que, ao acrescentar no art. 189º do CPP a expressão "*mesmo que se encontrem guardadas em suporte digital*", o legislador acaba por limitar os meios excecionais de investigação, sujeitando-os ao catálogo previsto no art. 187º nº1 do CPP e impede a sua investigação nos crimes em que a sua intromissão seria mais necessária, como nas situações de injúria ou coação[39].

---

[36] *Ibid.*, p. 185
[37] *Ibid.*, p. 185
[38] Acórdão do Tribunal da Relação de Coimbra, de 28 de Janeiro de 2009
[39] A este propósito *vg*. o Acórdão do Tribunal da Relação de Évora de 26 de Julho de 2007 (Proc. nº843/07-1). Segundo este acórdão, "o crime de acesso ilegítimo p.p. pelo art. 7º nº1 da Lei 109/91 de 17/08, ao qual corresponde, em abstrato, pena de prisão até 1 ano ou pena de multa até 120 dias, não se enquadra no catálogo de crimes previstos no art. 187º do CPP em relação aos quais é admissível a interceção e a gravação das conversações ou comunicações, daí que a obtenção dos referidos elementos seja legalmente inadmissível." Conclui o referido acórdão que é compreensível a "indignação do recorrente ao ser-lhe vedado o acesso a elementos essenciais à investigação em causa. Cabe, porém, ao legislador, se assim o entender, fazê-lo integrar no elenco do catálogo de crimes previstos no art. 187º do CPP, à semelhança do que acontece com crimes de pouca gravidade, como a injúria e a ameaça, quando cometidos através do telefone, integrados na alínea e) do mesmo preceito", o que acabou por não acontecer na Reforma do CPP, de 2007

Também Paulo Pinto de Albuquerque defende que a redação deste artigo dada pela alteração do CPP, em dois mil e sete, vedou a aplicação do correio eletrónico " (…) nos crimes onde ela mais se afigura necessária, tais como os crimes de ameaça e injúrias cometidas pelo correio eletrónico e ainda os crimes de dano informático, acesso ilegítimo, intercepção ilegítima e reprodução ilegítima de programa protegido, previstos na Lei n.º 109/91 de 17.8, em virtude da moldura penal destes crimes."[40]

Considerar que o correio eletrónico (e equiparáveis), enquanto meros ficheiros informáticos têm de ser subsumidos – na perspetiva do processo penal- ao regime das buscas e apreensões, significa, na prática, que, de forma a apreender suportes digitais resultantes de comunicações eletrónicas, teremos de apreender o suporte físico a elas inerente, neste caso, o computador. Todavia, como bem refere Rita Castanheira Neves, parece ainda existir a possibilidade de estabelecer um "paralelismo para as apreensões através de cópia dos suportes digitais em substituição da apreensão do computador com o que se encontra previsto no art. 183º do CPP"[41]. O mesmo será dizer que, para esta autora, as autoridades competentes podem decidir proceder à cópia integral ou parcial dos conteúdos presentes nos computadores para outros suportes, como CDs, DVDs, *pens*, discos rígidos ou outros aparelhos de armazenamento de dados, em substituição da apreensão no computador em si (art. 19º da Lei n.º 109/2009, de quinze de setembro), uma vez que este método de apreensão é equivalente à apreensão física propriamente dita.

Em virtude da possibilidade de apreensão de outros suportes físicos, como CDs, DVDs ou *pens*, que possibilitam o acesso a informação sensível e da grave ingerência que o seu acesso constitui para a esfera privada do indivíduo, a doutrina, preocupada em minimizar os riscos de uma ilegítima ingerência em comunicações eletrónicas e em respeitar as exigências dos princípios da necessidade e da proporcionalidade da prova, tem refletido a respeito da busca *online*, enquanto meio de prova em processo penal.

Parafraseando Manuel da Costa Andrade, podemos definir as buscas *online* como "o conjunto de procedimentos – diversificados tanto do ponto de vista das técnicas utilizadas como a direção das suas formas de intromissão e devassa que têm alguns momentos em comum. Trata-se, em geral, de aceder, de forma oculta e à distância, via

[40] ALBUQUERQUE, Paulo Pinto de - *Comentário ao Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, 2008, Anotação 3 ao art. 189º do CPP, p. 544
[41] NEVES, *op. cit*., p. 192

internet, aos dados contidos num computador, observá-los e, sendo caso disso, copiá-los em maior ou menor medida. O que pode acontecer sobre a forma de intromissão instantânea e descontinua ("espelho") ou de forma contínua, permitindo o registo das alterações ocorridas nos computadores-alvo (monitoring)."[42]

De facto, os agentes de investigação criminal podem realizar buscas a partir de outro terminal informático, de forma oculta, sem que o visado se aperceba que está a ser alvo de escuta. Mas, tal como as buscas tradicionais, também as buscas *online* teriam de ser sujeitas a regras, ficando subordinadas a determinados princípios, nomeadamente o principio da necessidade e proporcionalidade.

Entendemos que, em virtude da evolução tecnológica, impunha-se ao legislador que promovesse a alteração dos meios de obtenção de prova em processo penal, passando a consagrar as buscas *online* que, pelas suas especificidades, merecem um tratamento substancialmente diferente das buscas presenciais, tal como estão consagradas no CPP.

Atente ao facto das buscas *online* não estarem previstas como meio de obtenção de prova em processo penal no ordenamento jurídico português, a sua legalidade no âmbito da investigação criminal encontra-se inevitavelmente comprometida.

3.2.1.3. Da ingerência em tempo real do correio eletrónico (e equiparáveis): a necessidade de uma autonomização do regime.

No que concerne à ingerência em tempo real do correio eletrónico (enquanto ele ainda é comunicação) e de outras comunicações eletrónicas a ele equiparáveis, a doutrina divide-se.

Para Pedro Verdelho, por exemplo, é possível a interceção em tempo real do correio eletrónico e de outros meios a ele equiparáveis, nos mesmos termos em que a lei permite a realização de escutas telefónicas, aplicando-se, nestes casos, o regime das escutas telefónicas[43].

Por sua vez, Manuel da Costa Andrade[44] entende que, no caso da ingerência em tempo real do correio eletrónico e das demais comunicações eletrónicas, estamos perante

[42] ANDRADE, 2009, p. 153.
[43] VERDELHO, 2004b, *op. cit.,* p. 155
[44] ANDRADE, *op. cit.*, 184-187

intromissões nas telecomunicações, pelo que deve ser aplicado o regime das escutas telefónicas. Todavia, para este autor, o atual art. 187º do CPP precisa de uma reformulação. Assim, Costa Andrade propõe a substituição do capítulo das escutas telefónicas, no CPP, por um regime geral mais amplo, eliminando o art. 189º do referido diploma. Desta forma, no entendimento deste autor, tudo o que atualmente se encontra abrangido no art. 189º do CPP e que não é comunicação[45], deixaria de estar submetido a este regime repleto de incongruências. Acrescenta, ainda, que os "documentos" guardados no computador e provenientes de comunicações eletrónicas deviam ser submetidos ao regime das buscas e apreensões, e que as comunicações entre presentes deviam ter um regime mais exigente e seletivo, em comparação com o regime das intromissões nas telecomunicações.

Em sentido idêntico, Rita Castanheira Neves[46] é de opinião que as ingerências no correio eletrónico e demais comunicações eletrónicas equiparáveis deviam ter um regime autónomo e diferenciado do regime das escutas, devido à sua distinta natureza. Para esta autora, estes dois meios não podem ser equiparados, uma vez que reclamam de um grau de proteção constitucional diferente. Deve, por isso, ser exigida uma tutela mais forte no caso da palavra escrita, uma vez que há uma maior ponderação do emissor quando envia uma mensagem de correio eletrónico, no sentido em que dedica maior cuidado às palavras devido à perpetuação desse registo no tempo, do que quando comunica oralmente.

Por seu turno, Benjamim da Silva Rodrigues[47] propõe um novo regime, com um capítulo autónomo no CPP epigrafado de "Monitorização dos Fluxos Informacionais e Comunicacionais", onde existiriam três contextos de intervenção distintos, a saber, as redes postais públicas, as redes de serviços e comunicações eletrónicas e o ambiente não digital. Na sequência desta sua proposta, defende este autor que deveriam ser eliminados os artigos 179º e 180º do CPP, bem como deveriam ainda ser introduzidos artigos dedicados às perícias informático-digitais, bem como ao exame e às buscas informático-digitais.

A este respeito, importa ainda sublinhar as incoerências da articulação legal do art. 189º do CPP e do art. 18º da Lei n.º 109/2009, que se traduziram em diversas questões,

[45]Nomeadamente as intromissões nos "documentos" guardados no computador resultantes de comunicações eletrónicas e a interceção e gravação de comunicações entre presentes, de que temos vindo a falar

[46] NEVES, *op. cit.*, pp.172-173. A este respeito, *vg*. ainda pp. 206-208

[47] RODRIGUES, 2008, *op.cit*, p. 540

nomeadamente a possibilidade de manutenção em vigor do art. 189º do CPP, em coexistência com o art. 18º da Lei n.º 109/2009, e os casos de aplicação de um e de outro. Sobre estas questões teremos a oportunidade de tecer algumas observações no capítulo 4.2.2.

3.2.1.4. Da "*interceção das comunicações entre presentes*"

No âmbito da reforma do CPP de dois mil e sete, o legislador decidiu aditar ao art. 189º uma terceira parte, onde estabeleceu a extensão do regime das escutas telefónicas à "*interceção das comunicações entre presentes*", o que provocou duras e merecidas críticas por parte da doutrina.

Ora, como se sabe, as telecomunicações e as comunicações entre presentes não podiam ser mais díspares. Se, por um lado, nas telecomunicações, a transmissão da mensagem é feita através da palavra falada e/ou escrita a um destinatário que não está presente, por outro lado, nas comunicações entre presentes, como o próprio nome indica, a palavra falada é transmitida diretamente ao recetor que está presente no mesmo espaço físico, dispensando, por isso, a utilização de qualquer aparelho técnico de transmissão. É isto que distingue as comunicações entre presentes, das demais comunicações.

Partindo desta premissa, não se compreende, por isso, a opção do legislador em reconduzir a interceção das comunicações entre presentes ao regime das escutas telefónicas.

É altamente censurável esta opção, uma vez que, como alerta Manuel da Costa Andrade, a "interceção, gravação e posterior audição e utilização"[48] da comunicação entre presentes "representam um potencial de devassa e danosidade social claramente superior (comparativamente às intromissões nas telecomunicações)."[49] Nesta linha de raciocínio, este autor defende que a interceção das comunicações entre presentes devia gozar de um regime "mais consistente e, na perspetiva da intromissão, mais exigente e seletivo (do que o regime das intromissões nas telecomunicações)."[50]

[48] ANDRADE, *op.cit*., 2009, p. 186
[49] *Ibid*.,p. 186
[50] *Ibid,* p. 186

Ao remeter para o mesmo artigo do CPP duas realidades completamente distintas – as telecomunicações e as comunicações entre presentes - o legislador esvaziou-o de sentido.

Paulo Pinto de Albuquerque é também uma das vozes críticas relativamente à opção do legislador em submeter as conversas entre presentes ao regime das escutas telefónicas. Para este autor, o legislador não distinguiu "entre as conversações privadas ditas entre presentes no domicilio ou fora dele, e portanto, incluindo quer as conversações ditas em casa habitada quer as tidas em via pública ou em qualquer outro edifício ou local de acesso público ou restrito."[51] Refere, ainda, este autor, que o direito à privacidade, constitucionalmente consagrado no art. 26º e 35º da Constituição da República Portuguesa (doravante CRP) "impõe restrições a estas interferências"[52], pelo que, a interceção de comunicações entre presentes, no domicilio deve ser considerada inconstitucional.

Atendendo às implicações no âmbito dos direitos fundamentais que a extensão do regime das escutas telefónicas à "*interceção das comunicações entre presentes*", Manuel da Costa Andrade[53], Benjamim Silva Rodrigues[54] e André Lamas Leite[55] defendem que o legislador deveria ter consagrado um regime autónomo para a interceção das comunicações entre presentes, de forma a solucionar, como bem sintetiza Rita Castanheira Neves, "ausências e incoerências legislativas que atualmente assombram o panorama da lei adjetiva penal"[56].

Por fim, refira-se que a Reforma do CPP, de dois mil e sete, aditou ainda um n.º2 ao art. 189º do CPP, estendendo, desta forma, o regime das escutas também à localização celular e dados de tráfego. Contudo, a redação (infeliz) do n.º2 deste preceito, que reconduziu a localização celular ou dados de tráfego ao regime das escutas telefónicas, deixa muito a desejar. Não nos alongaremos em relação a este ponto, uma vez que este não é o tema central do nosso trabalho.

Em virtude do atrás exposto e em jeito de conclusão, resulta clara a irrefletida redação do art. 189º do CPP que, ao reconduzir o correio eletrónico ao regime das escutas

[51] ALBUQUERQUE, *op. cit*., Anotação 4 ao art. 189º do CPP, p. 544
[52] *Ibid*., p. 544
[53] ANDRADE, *op. cit*., 2009, p. 186
[54] RODRIGUES, *op. cit*., 2008, pp. 439-440
[55] LEITE, André Lamas - Entre Péricles e Sísifo: o novo regime legal das escutas telefónicas, 2007, p. 19
[56] NEVES, *op. cit.,* p. 159

telefónicas, ao invés de ter colmatado algumas lacunas do anterior código, suscitou ainda mais questões.

3.2.2. A Lei da Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas (Lei n.º 32/2008)

Com a Reforma do CPP, o legislador perdeu uma oportunidade para inserir neste diploma as medidas previstas pela Diretiva n.º 2006/24/CE do Parlamento Europeu e pelo Conselho, de quinze de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicação[57].

Não obstante ter existido preocupação por parte do legislador em estabelecer os requisitos de admissibilidade e as formalidades no acesso, conservação e transmissão dos dados de tráfego e localização, bem como dos dados relevantes para a identificação do utilizador, garantindo a investigação e repressão de crimes graves de forma mais célere, na nossa opinião, a transposição da Diretiva n.º 2006/24/CE do Parlamento Europeu e do Conselho, de quinze de março, nestes moldes, acabou por ser um verdadeiro desastre, como nos propomos aprofundar em seguida.

Da análise do n.º2 do art. 9º da Lei n.º 32/2008 resulta claro que só o MP ou OPC competente podem requerer a transmissão de dados relativos a suspeito/arguido, à pessoa que sirva de intermediário e relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido, ou à própria vítima, desde que ela tenha dado o seu consentimento para tal (n.º 3 do mesmo artigo).

Todavia, a decisão de transmitir os dados referentes às categorias de pessoas elencadas no n.º3 do art. 9º apenas está ao alcance do Juiz de Instrução Criminal (doravante JIC) que, caso entenda que tais dados são indispensáveis para a descoberta da verdade, ou que a mesma é impossível ou muito difícil sem eles, autoriza a transmissão

[57] A transposição desta diretiva para o ordenamento jurídico português viria a ser feita pela Lei n.º 32/2008, de dezassete de julho, uma Lei marcada por incoerências várias, como aprofundaremos neste ponto

de dados, através de despacho fundamentado. Se, por outro lado, entender que estes requisitos não se encontram devidamente preenchidos, vedará a transmissão dos dados.

Assim, o JIC apresenta-se como uma figura nuclear no processo, na medida em que a transmissão de dados sensíveis terá de passar pelo seu crivo, nos termos do art. 3º e art. 9º da Lei n.º 32/2008, de dezassete de julho.

Atendendo à danosidade social indissociavelmente ligada à transmissibilidade dos dados, a decisão do JIC tem necessariamente de ser pautada pelo princípio da adequação, necessidade e proporcionalidade (cf. art. 9º n.º 4 da Lei n.º 32/2008).

O art. 6º da Lei n.º 32/2008, por outro lado, diz respeito ao período de conservação dos dados. De acordo com este preceito, os dados (relativos às pessoas devidamente elencadas no n.º 3 do art. 9º) têm de ser conservados por um período máximo de um ano.

No momento em que os dados deixem de ser necessários no decurso da investigação, o JIC determina a destruição dos mesmos nos termos do art. 10º n.º1 e 2 da referida Lei.

Da contextualização apresentada, é nosso entendimento que o legislador português não foi feliz na redação da lei, duplicando desnecessariamente os regimes em matéria de prova ao consagrar, por um lado, as normas gerais no CPP e por outro lado, as normas especiais na Lei n.º 32/2008[58].

Assim, entendemos, na esteira de Lima Cancela, que o problema teria sido solucionado "se o acesso aos dados se regulasse pela lei geral, autonomizada da legislação extravagante, que apenas regularia as questões técnicas à sua conservação preventiva, mantendo-se a centralidade normativa da lei processual penal."[59] Só desta forma a duplicação de regimes poderia ser evitada.

[58] Cf. CORREIA, *op. cit.*, p. 40 e ss
[59] CANCELA, *Alberto Gil Lima - A prova digital: Os meios de obtenção de prova na Lei do Cibercrime,* 2016, p. 28

3.2.3. Da Lei da Cibercriminalidade Informática (Lei n.º 109/91) à atual Lei do Cibercrime (Lei n.º 109/2009 de 15 de Setembro)

A Lei n.º 109/91 de dezassete de agosto, em vigor desde mil novecentos e noventa e um, e vulgarmente conhecida como Lei da Cibercriminalidade Informática, foi criada com o objetivo de regular e combater eficazmente a cibercriminalidade.

Com a Lei n.º 109/91, de dezassete de agosto, o legislador português procedeu à introdução de diversos conceitos, de entre os quais destacamos, pela pertinente relação com o tema aqui em discussão, o catálogo de crimes ligados à informática, como a "falsidade informática, o dano relativo a dados ou programas informáticos, a sabotagem informática, o acesso ilegítimo, a interceção ilegítima, a reprodução ilegítima de programa protegido."[60]

Contudo, com o passar do tempo e com o aparecimento de novas formas de atuar propiciadas pelo incremento dos meios informáticos, este diploma veio a revelar-se insuficiente e deficitário.

Neste contexto e para dar resposta às novas exigências nacionais e internacionais, tornava-se necessário unir esforços e uniformizar práticas de prevenção e repressão contra a criminalidade tecnológica.

Em dois mil e um, com a ratificação portuguesa à Convenção sobre o Cibercrime do Conselho da Europa e a necessária transposição da Decisão Quadro n.º 2005/222/JAI, do Conselho, de vinte e quatro de fevereiro, o direito interno foi forçado a adaptar-se à legislação internacional.

Todavia, pressionado pelas exigências europeias[61], o legislador português precipitou-se ao criar este diploma avulso – a Lei n.º 109/2009- no qual "(…) condensou num só diploma legislativo todas as normas respeitantes à cibercriminalidade, aglutinando normas de direito penal material (sobretudo criando tipos de crime), normas processuais (que são exceção ás regras gerais do CPP) e ainda normas respeitantes à cooperação penal internacional (que complementam as disposições da Lei da Cooperação

[60] *Ibid.*, p. 18
[61] A Decisão- Quadro 2005/222/JAI deveria ter sido transposta em 16/03/2007 e o prazo de implementação da Convenção do Cibercrime terminava em 23/01/2001

Judiciária Internacional em matéria penal- Lei n.º 144/99 de 31/08 com as sucessivas alterações).”[62]

De forma a uma melhor compreensão desta temática, propomos uma análise da Lei n.º 109/2009, de quinze de setembro.

Neste diploma legal encontramos, simultaneamente, disposições normativas que regulam a preservação expedita de dados (art. 12º), a revelação expedita de dados de tráfego (art. 13º), a injunção para apresentação ou concessão do acesso a dados (art. 14º), a pesquisa de dados informáticos (art. 15º), a apreensão de dados informáticos (art. 16º), a apreensão de correio eletrónico e registo de comunicações de natureza semelhante (art. 17º), a interceção de comunicações (art. 18º), as ações encobertas (art.19º) e ainda a regulação da cooperação internacional (art. 20º ao art. 26º).

Em virtude da extensão e complexidade do diploma legal surgiram dissensos na doutrina, como daremos conta.

Assim, para Paulo Dá Mesquita, “as regras de direito probatório previstas no diploma não são meras normas processuais sobre cibercrimes ou sequer apenas relativas a crimes praticados em sistemas informáticos, mas correspondem a um regime consideravelmente mais abrangente sobre prova eletrónica em processo penal aplicável a qualquer crime.”[63]

Ou seja, para este autor, as medidas processuais previstas nos artigos 12º a 17º da Lei n.º 109/2009, aplicando-se a todos os crimes informáticos ou relativamente aos quais seja necessário proceder à recolha de prova em suporte eletrónico, são excessivamente amplas.

Neste sentido, entendemos, tal como Renato Lopes Militão, que a Lei n.º 109/2009, ao consagrar “um regime processual geral de obtenção de prova digital, potencialmente dirigido a todos os crimes” [64] deveria ter sido integrada no CPP.

Uma outra incongruência da referida Lei diz respeito ao n.º 2 do art. 11º. Segundo este preceito, “as disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho”. Comparando um e outro diploma, podemos

[62] VERDELHO, Pedro - A nova lei do cibercrime, 2009, pp. 718-719
[63] MESQUITA, Paulo Dá - *Processo Penal, Prova e Sistema Judiciário*, 2010, p. 98. *Vg*., ainda, Acórdão do Tribunal da Relação de Coimbra de 26 de Fevereiro de 2014. Proc. nº 559/12.0GBOBR-A.C1
[64] MILITÃO, *op. cit.,* p. 273

facilmente constatar que os regimes são contraditórios. Assim, se da análise dos artigos 12º, 13º e 14º da Lei n.º 109/2009 resulta claro que a preservação de dados por parte do fornecedor de serviço só pode ser ordenada por entidade judiciária ou quando existir urgência ou perigo na demora, sendo que o fornecedor de serviço a quem a prestação for ordenada terá posteriormente de indicar à autoridade judiciária ou OPC outros fornecedores de serviço através dos quais a comunicação tenha sido efetuada e, por fim, que os fornecedores de serviços estão ainda obrigados a comunicar os dados ao processo ou permitir acesso aos mesmos, sob pena de punição por desobediência. Por outro lado, se atendermos ao art. 9º da Lei n.º 32/2008, que determina que a transmissão dos dados de tráfego e localização "só pode ser autorizada por despacho fundamentado do JIC se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves", previstos no art.2º nº1, alínea g) da referida lei, verificamos, também, que existe uma incompatibilidade dos dois diplomas legais.

De forma a resolver o problema com que nos deparamos, Rita Castanheira Neves propõe a demarcação "de campos de aplicação distintos para a Lei n.º 32/2008 e para a Lei n.º 109/2009."[65] Assim, esclarece a autora, "se aquela primeira se aplica à investigação de crimes "graves"- tal como definido na alínea g) do nº 1 do artigo 2º - procedendo-se aqui à obtenção de dados de tráfego e localização através das mencionadas exigências do art.9º, já a segunda lei só se aplicará no caso de a investigação criminal em curso dizer respeito a crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico."[66]

Contudo, como bem observa Vanessa Chagas Cardoso[67], não se encontra prevista a possibilidade de existirem crimes graves, cometidos por meio de um sistema informático ou em relação aos quais seja necessário a recolha de prova em suporte eletrónico.

Ora, havendo coincidência entre os dois diplomas importa perceber quando aplicar um e outro.

---

[65] NEVES, *op. cit*, p. 237
[66] *Ibid*., p. 237
[67] CARDOSO, Vanessa Chagas - *Telecomunicações e prova em processo penal : das escutas telefónicas à intromissão nas comunicações electrónicas*, 2014, p. 44

Como sabemos, é impossível cumular os dois regimes quando as disposições neles constantes coincidem. Nestes casos, aplica-se princípio da "*lex posteriori derogat lex priori*", ou seja, neste caso, a Lei n.º 109/2009 revogaria a Lei n.º 32/2008.

No que concerne aos artigos 17º e 18º da Lei n.º 109/2009, destacamos a inovação do legislador que, aquando da sua redação, optou por dar um tratamento diferente para a ingerência no correio eletrónico que se encontra armazenado em suporte digital e aquele que se encontra em transmissão. Não sendo o CPP suficientemente explicito nesta matéria, é de aplaudir esta opção em estabelecer artigos diferentes para ambas as situações.

O art. 19º da Lei aqui em apreço admite o recurso a ações encobertas nos termos da Lei n.º 101/2001 de 25 de Agosto, no decurso de inquérito relativo a crimes "cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos". Pese embora a pertinência das questões e matérias envolvidas, cingimo-nos neste trabalho, pelas limitações textuais impostas, a abordar apenas algumas questões mais relevantes.

De facto, são várias as vozes discordantes no que respeita ao art. 19º da Lei n.º 109/2009.

Paulo Dá Mesquita entende que, se, por um lado, o legislador ampliou de forma contundente o catálogo de crimes previsto no artigo 2.º do Regime Jurídico das Ações Encobertas, por outro, passa a prever uma medida excecional para um leque amplo de crimes, sem aprofundar normativamente os princípios da proporcionalidade e da necessidade[68].

Susana Aires de Sousa, por seu turno, refere a este propósito, que as condutas a adotar pelo agente infiltrado e pelo agente provocador são diferentes. Assim, é importante distinguir o papel de um e de outro para determinar "a responsabilidade penal substantiva

[68] MESQUITA, *op. cit.*, p. 126

daqueles sujeitos" e fazer o "tratamento jurídico processual das provas obtidas e recolhidas"[69]. Neste sentido, considera a autora que as provas obtidas pelo agente infiltrado devem ser admitidas, mas aquelas que forem obtidas pelo agente provocador, são inválidas e feridas de nulidade, uma vez que representam uma enorme agressão aos seus direitos fundamentais.

Ainda a este respeito, sublinhamos a posição de Paulo Dá Mesquita, que afirma que "o n.º2 do art. 19º, aprofundando a incongruência sistemática consagra-se uma norma espúria no ordenamento jurídico português ao prever, sem qualquer outro enquadramento, "o recurso a meios e dispositivos informáticos em ações encobertas", podendo "estar-se, por esta via, a abrir-se, sem suficiente ponderação (ou freios claros) a porta à interceção de comunicações para fins de prevenção (…), constitucionalmente incompatível com o disposto no art. 34º da Constituição."[70]

Já para Costa Andrade, o legislador devia ter incluído uma terceira figura, por ele designada de "Homem de Confiança", e que seria um terceiro que "disfarçadamente se introduzem naquele submundo ou com ele entram em contato; e que quer se limitem à recolha de informações (…), quer vão ao ponto de provocar eles próprios a prática do crime" [71] atuam no meio criminoso, sob orientação do OPC.

No âmbito da cooperação internacional, destacamos o artigo 22º da Lei n.º 109/2009, relativo à preservação e revelação expedita de dados informáticos em cooperação internacional; o artigo 24º, relativo à pesquisa, apreensão e divulgação de dados informáticos em cooperação internacional; e o artigo 25º, relativo ao acesso das autoridades estrangeiras competentes a dados informáticos armazenados em sistemas informáticos localizados em Portugal e a receção e acesso destas autoridades, sem pedido de autorização às entidades portuguesas competentes, a dados informáticos.

Para Renato Lopes Militão, a Lei n.º 109/2009 veio dotar os OPC de poderes acrescidos no que se refere à preservação, pesquisa e apreensão de dados informáticos, pois com a entrada em vigor deste diploma, o OPC passou a dispor de "competência própria para:- ordenar a preservação expedita de dados informáticos (art. 12º n.º2), -proceder à pesquisa de dados informáticos (art. 15º n.º3); -efetuar a apreensão de dados

[69] SOUSA, Susana Aires de - Agent Provocateur e meios enganosos de prova. Algumas reflexões, 2003, p. 1235
[70] MESQUITA, *op. cit.*, p. 127
[71] ANDRADE, Manuel da Costa - *Sobre as proibições de prova em processo pena*l, 1992, p. 220

informáticos (art. 16º nº2)."[72] Este autor sublinha ainda o facto de este diploma permitir que o OPC "ordene a preservação, pesquisa ou apreensão de dados informáticos mediante delegação da autoridade judiciária competente (art. 12º nº2, 15º nº1, 16º n.º1 e 22º n.º4)."[73]

No que concerne a este ponto, Benjamim da Silva Rodrigues adverte para a possibilidade do presente diploma legal "resvalar para uma nova forma de "terrorismo societário" (mediante alienação do fim) que tem a especificidade de ser, de forma algo contraditória, levado a cabo pelo Estado Português."[74]

Também o art. 27º da referida lei vem a revelar incongruências várias e a suscitar críticas fundamentadas. Salientamos a opinião de Vera Marques Dias, para quem "a diversidade de ordens jurídicas existentes e a qualificação diferente de ilícito é outro dos problemas, pois leva a que à mesma infração sejam aplicadas sanções diferentes, ou mesmo que uma conduta seja crime num país e noutro não (…)."[75] A autora dá especial ênfase à importância de se delimitar a lei aplicável, particularmente quando se geram dúvidas em relação a quando deve ser aplicada a lei portuguesa. Nas palavras da autora: "No caso do cibercrime coloca-se a dúvida de saber se aplica a lei do país onde está o servidor utilizado pelo infrator, onde o infrator praticou a infração, onde reside o infrator, ou onde o(s) resultado (s) da sua conduta é (são) produzido(s) (…)."[76]

Em termos globais, podemos afirmar que, não obstante a Lei n.º 109/2009 ser uma lei inovadora no que concerne ao regime de prova digital, a decisão do legislador em criar um novo diploma que se sobreporia à Lei n.º 32/2008, levou a diversas incongruências normativas. Neste sentido, Alberto Gil Lima Cancela afirma que "a Lei do Cibercrime viria a agravar dilemas técnico-legislativos já existentes, levando a um aumento da agressão na investigação criminal, em comparação com a investigação com recurso às chamadas "provas tradicionais"[77].

Costa Andrade também é muito crítico na avaliação que faz da Lei n.º 109/2009, declarando que "ao ignorar as matérias de criminalidade informática, o legislador falhou

[72] MILITÃO, *op. cit.,* p. 280
[73] *Ibid.*, p. 280
[74] RODRIGUES, 2008, p. 36
[75] DIAS, *op. cit*, p.72
[76] *Ibid.,* p. 72
[77] CANCELA, *op. cit*., p. 65

ao aproximar o ordenamento jurídico português dos restantes [aumentando] o fosso da divergência face aos avanços de outros ordenamentos jurídicos."[78]

[78]ANDRADE, 2009, p. 337

4. O CORREIO ELETRÓNICO: CONFRONTO ENTRE OS VÁRIOS DIPLOMAS

Em matéria de prova digital existem, além do CPP, outros dois diplomas avulsos, a saber, a Lei n.º 32/2008, de dezassete de julho e a Lei n.º 109/2009, de quinze de setembro, o que dificulta a interpretação e consequente aplicação desta matéria por parte do legislador[79].

Uma das questões mais controvertidas prende-se com a articulação da Lei n.º 32/2008 e da Lei n.º 109/2009, com o regime previsto no artigo 189º do CPP, uma vez que, tal como bem afirma Catarina Rodrigues Santos Costa, "a Lei n.º 32/2008 e, temporalmente após, a Lei do Cibercrime, revogaram, ainda que tacitamente, parcelas de vulto da matriz do regime do art. 189.º do CPP, reduzindo em muito o seu âmbito de aplicação inicial, sobrepondo-se as leis extravagantes àquele regime geral, que só subsiste no que não foi depois especialmente regulado por elas."[80]

Para além disso, refiram-se, também, as críticas a apontar ao legislador que, sabendo das diferenças técnicas e diversidade de objeto afeto aos três diplomas, optou por manter aquilo que Costa designa como "teia dispersa e incoerente"[81].

Chegados aqui, debruçar-nos-emos, agora, com maior detalhe, sobre a articulação destes três diplomas legais, procurando, desta forma, contribuir para a formação de posições mais solidamente sustentadas.

4.1. A Lei n.º 32/2008 e a Lei n.º 109/2009

Existe uma querela doutrinária no que respeita à articulação entre a Lei n.º 32/2008 e a Lei n.º 109/2009, surgindo duas posições antagónicas.

A primeira tese, defendida por uma corrente doutrinária minoritária, argumenta que a Lei n.º 109/2009, mais concretamente, a conjugação dos arts. 11º, 12º, 13º, 14º, 16º e 18º implica a revogação do art. 9º da Lei n.º 32/2008.

---

[79] Segundo João Conde Correia, "esta trilogia para além de acentuar o atual paradigma de descodificação e de negar a desejável centralidade normativa do Código de Processo Penal, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático." (CORREIA, João Conde, *op. cit.*, p. 139)

[80] COSTA, Catarina Rodrigues Santos - *As proibições de prova e a prova digital – aproximação aos lugares-comuns de um instituto clássico em face de uma nova realidade*, 2017, p. 109

[81] *Ibid.,* p. 94

Esta doutrina, defendida por Paulo Dá Mesquita, e na qual, com o devido respeito, não nos revemos, aponta vários argumentos no sentido de apenas podermos considerar a Lei n.º 32/2008 em matéria de "estabelecimento dos deveres dos fornecedores de serviços e prestação desses dados"[82], uma vez que esta matéria não é regulada pela Lei n.º 109/2009.

Assim, para os defensores desta posição, caso esta matéria se encontrasse regulada nos dois diplomas - que não são complementares - manter ambos os regimes "implicaria uma oneração dos crimes mais graves" [83].

Posição diferente é a defendida por Rita Castanheira Neves[84]. Para esta autora, a intenção do legislador com a remissão do n.º 2 do art. 11º da Lei n.º 109/2009 para a Lei n.º32/2008 seria a de articular ambas as leis. Mais entende que, com a entrada em vigor destes dois diplomas legais extravagantes, há uma redução de protagonismo do CPP em matéria de investigação criminal, deparando-se o intérprete com a difícil tarefa de aplicar uma (Lei n.º 32/2008) ou outra (Lei n.º109/2009), face a uma situação concreta.

4.2. A Lei n.º 109/2009 e o Código de Processo Penal

Com a Reforma do CPP, de dois mil e sete, surge consagrado no art. 189º do CPP a extensão do regime das escutas telefónicas. Como já foi referido anteriormente, no n.º1 deste preceito podemos distinguir duas realidades distintas: por um lado, a interceção e registo de comunicações ou conversações realizadas (em tempo real) através de meio técnico diferente do telefone e, por outro, as comunicações ou conversações eletrónicas, que se encontrem armazenadas em suporte digital, e nas quais se incluem o correio eletrónico.

O regime de recolha de prova em ambiente digital viria a sofrer alterações com a entrada em vigor da Lei n.º 109/2009, conhecida como Lei do Cibercrime, em dois mil e nove e, como bem refere Paulo Dá Mesquita, "o correio eletrónico e as comunicações de natureza semelhante transmitidas através de sistemas informáticos passaram (desde 2009) a compreender, pelo menos, duas constelações com sedes normativas distintas: a

[82] MESQUITA, Paulo Dá*, op. cit.,* p. 123
[83] DIAS, Vera Marques, *op. cit*., p. 19
[84] NEVES, Rita Castanheira, *op. cit.,* pp. 284-285

apreensão da correspondência do Código de Processo Penal e um regime específico de interceção e registo de comunicações de dados informáticos."[85]

Existindo duas fontes normativas – a Lei n.º 109/2009 e o CPP- que regulam o modo de obtenção da prova digital, o intérprete é confrontado com questões de interpretação no que concerne aos respetivos campos de aplicação. Qual deve ser o âmbito de aplicação do n.º1 do art. 189º do CPP?

De seguida, debruçar-nos-emos sobre esta questão que, por constituir uma dúvida relevante, merece a nossa atenção e estudo em subcapítulo específico.

4.2.1. O regime jurídico aplicável à ingerência nas comunicações armazenadas em suporte digital: críticas

Até à entrada em vigor da Lei n.º 109/2009, era corrente maioritária na doutrina e jurisprudência que as mensagens de correio eletrónico ou outras de natureza semelhante que tivessem sido lidas e armazenadas em suporte digital deviam ser objeto de tratamento idêntico ao da "carta em papel que, tendo sido recebida pelo correio e aberta, foi guardada em arquivo pessoal"[86], ou seja, havia uma equiparação do correio eletrónico à correspondência tradicional[87].

A Lei n.º 109/2009 veio alterar o cenário legislativo em matéria de prova, uma vez que com este diploma as ingerências nas comunicações armazenadas em suporte digital passaram a dispor de maior tutela face aos arquivos físicos. Esta opção do legislador foi severamente criticada por alguns autores, entre eles Manuel da Costa Andrade[88] para quem não faz sentido existir uma maior proteção das ingerências nas comunicações armazenadas em suporte digital, por não estarmos perante um ato comunicacional, como equivocamente se pensa, mas perante um produto do ato comunicacional e que, por isso, está fora do âmbito das telecomunicações.

---

[85] MESQUITA, *op. cit.*, p. 119

[86] Acórdão do Tribunal da Relação de Guimarães, de 12 de Outubro de 2009 (Proc. nº 1396/08.1PBGMR). No mesmo sentido, *vg.* Acórdão do Tribunal da Relação de Lisboa, de 15 de Julho de 2008 (Proc. n.º 3453/2008-5) e Acórdão do Tribunal da Relação do Porto de 27 de Janeiro de 2010 (Proc. n.º 896/07.5412/08.9TDLSB-A.L1-5)

[87] Posição defendida por Pedro Verdelho (VERDELHO, Pedro - A obtenção de Prova em Ambiente Digital. 2004a)

[88] ANDRADE*, op. cit.*, 2009, pp. 156-160

Feito este breve enquadramento da temática que nos propomos tratar, cumpre-nos agora analisar o que mudou com a entrada em vigor da Lei n.º 109/2009, de quinze de setembro, averiguando da harmonização do art. 17º deste diploma, com o art. 189º do CPP.

Como é consabido, o art. 189º nº 1 do CPP prevê o regime da interceção e gravação de comunicações telefónicas quando esteja em causa a intromissão nas comunicações ou conversações armazenadas em suporte digital. Contudo, o art.17º da Lei n.º 109/2009, que versa sobre a mesma matéria, estabeleceu uma solução legal diversa para a ingerência nas comunicações armazenadas em suporte digital.

Diz-nos o art. 17º da referida Lei que "*o juiz poderá autorizar ou ordenar, por despacho, a apreensão"* de comunicações eletrónicas armazenadas em suporte digital, quando as mesmas sejam de *"grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente, o regime da apreensão da correspondência previsto no Código de Processo Penal.*" Esta diligência pode ser utilizada em processos relativos a crimes que estejam legalmente previstos, cometidos através de sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (art. 11º nº1 da mesma lei).

Enquanto que a Lei n.º 109/2009, no seu art. 11º n.º1, estabelece um leque de crimes mais amplo, ao qual é aplicado o regime de apreensão de correio eletrónico ou registos de natureza semelhante, deparamo-nos com uma situação diversa no nº 1 do art. 189º do CPP, em que apenas é permitido o recurso a esta diligência no âmbito de crimes elencados no n.º 1 do art. 187º e durante a fase de inquérito "*se houver razões para crer que a diligencia é indispensável para a descoberta da verdade, ou que a prova seria, de outro forma, impossível ou muito difícil de obter*".

Outro ponto divergente entre ambos os preceitos é o facto de, no art. 17º da Lei n.º 109/2009, a diligência ter de ser ordenada por um juiz, caso este entenda que é de "*grande interesse para a descoberta da verdade ou para a prova*". Se já existiam dúvidas acerca desta matéria, com a menção no final do art. 17º, onde se refere ser aplicável "*o regime da apreensão de correspondência previsto no Código de Processo Penal"*, mais dúvidas surgiram.

Urge, assim, tentar responder à questão que se coloca de saber qual deve ser o regime processual aplicado quando esteja em causa a intromissão em comunicações

eletrónicas armazenadas em suporte digital: deve ser aplicado o art. 17º da Lei nº 109/2009 ou, por outro lado, deve ser aplicado o art. 189º nº1 do CPP?

Segundo Paulo Dá Mesquita, o art. 17º da Lei n.º 109/2009 foi "o primeiro passo da direta revogação de algumas implicações do regime do Código de Processo Penal sobre intromissão em comunicações."[89]

No entender deste autor, "apesar da redação pouco clara (do art. 17º), a remissão para as regras de processo penal sobre a apreensão da correspondência, parece implicar que a mesma reconduz o intérprete à teleologia do regime processual sobre a apreensão da correspondência."[90] Por outras palavras, para este autor, o regime da apreensão de correio eletrónico e os registos de comunicação de natureza semelhante devem ser regulados pelo art. 17º da Lei n.º 109/2009 e apenas subsidiariamente pelos artigos 179º e 252º, ambos do CPP.

Em sentido contrário, considera Pedro Verdelho que devemos aplicar nestes casos o art. 189º do CPP que, por sua vez, remete para o regime da apreensão da correspondência eletrónica, elencado nos artigos 179º e 252º do CPP[91].

Mais refere este autor, que o regime da apreensão de correspondência previsto no art. 179º do CPP não deve ser aplicado na sua totalidade ao art. 17º da Lei n.º 109/2009, uma vez que a intervenção do juiz só pode ocorrer após apreensão das mensagens de correio eletrónico e registos de comunicação de natureza semelhante[92].

No mesmo sentido, Rita Castanheira Neves vem referir que o juiz deve ser "o primeiro a tomar conhecimento do conteúdo do correio eletrónico e demais registos de comunicações apreendido, mandando-o juntar ao processo se o considerar relevante."[93] No entanto, considera esta autora que seria prudente que se exigissem "estritos critérios

---

[89] MESQUITA, *op. cit.*, p. 117
[90] *Ibid.*, p. 118
[91] VERDELHO, *op. cit.,* 2009, p. 745
Cf. Igualmente José Mouraz Lopes aponta no sentido de que o correio eletrónico deve ser tratado como correspondência tradicional (LOPES, José Mouraz - *Garantia Judiciária no Processo Penal*, 2000). Em sentido oposto, *vg*. Rogério Bravo (BRAVO, Rogério - Da não equiparação do correio eletrónico ao correio tradicional de correspondência por carta. 2006). Segundo este autor, as mensagens de correio eletrónico não podem ser equiparadas à correspondência tradicional, uma vez que aquilo que carateriza a "correspondência-carta" é o facto de ser um objeto, corporizado e fechado quando remetido (…) ao contrário e por natureza, uma mensagem de "correio eletrónico", nunca é, nem nunca está "fechada (…)". (*ibid.*, p. 212)
[92] VERDELHO, *op. cit.*, 2009, pp. 745-746
[93] NEVES, *op. cit.*, p. 275

de abrangência, apenas apreendendo os e-mails que se afigurem realmente determinantes para a prova"[94], pois só assim poderá a diligência revelar-se eficaz.

Apesar das dúvidas que continuam a existir em torno desta matéria, a jurisprudência tem optado por tentar harmonizar os dois diplomas."[95]

4.2.2. O regime da interceção e registo de comunicações eletrónicas em tempo real

Até ao ano de dois mil e nove, o regime da interceção e registo de comunicações eletrónicas em tempo real encontrava-se regulado no CPP, sendo-lhe aplicável o mesmo regime da interceção e gravação de comunicações telefónicas (art. 187º do CPP).

Com a entrada em vigor da Lei n.º 109/2009 surgiu um regime específico para a interceção e registo de comunicações eletrónicas, com suporte legal no art. 18º da referida Lei.

O art. 18º da Lei n.º 109/2009 constitui uma verdadeira inovação uma vez que, "acabou por legitimar o recurso ao regime da interceção de comunicações (eletrónicas) em processos relativos a crimes, que até 2009, não eram permitidos."[96]

Não obstante o que foi atrás referido, entendemos que o legislador, nas palavras de Maria Joana Marques, na redação do n.º4 do art. 18º da Lei n.º 109/2009, ficou aquém do que era exigível, uma vez que se limitou a transpor para a Lei do Cibercrime, o regime relativo à interceção de comunicações, previsto no CPP.

Apesar de estarmos perante uma interceção de comunicações em ambos os casos, a verdade é que o objeto é distinto. Assim, e como resume Lima Cancela, se por um lado, "os artigos 187º e seguintes do Código de Processo Penal regulam a interceção e gravação de comunicações telefónicas. Por sua vez, o artigo 18º regula a interceção e registo de comunicações eletrónicas."[97]

---

[94] *Ibid.*, p. 275
[95] *Vg.* o Acórdão do Tribunal da Relação de Lisboa, de 11 de Janeiro de 2011 (Proc. n.º 5412/08.9TDLSB-A.L11-5)
[96] MARQUES, Maria Joana Xara-Brasil, *Os meios de obtenção de Prova na lei do Cibercrime e o seu confronto com o Código de Processo Penal*. 2014, p, 41
[97] CANCELA, *op. cit*, p. 42

Na opinião de Paulo Pinto de Albuquerque[98] e de Pedro Verdelho[99], o art. 189º nº1 do CPP deve manter-se em vigor, uma vez que, como explicita Pedro Verdelho, a Lei n.º 109/2009 apenas institui um "regime especial, destinado a ser aplicado em casos específicos, como resulta do respetivo artigo 11º." [100]

Também Rita Castanheira Neves[101] considera que devemos aplicar o art. 189º n.º1 do CPP. A autora alerta, contudo, para o facto de, estando em causa a recolha de prova informática, termos de recorrer à Lei n.º 109/2009, o que deixa pouco campo de aplicação para o art. 189º do CPP.

Por seu turno, Paulo Dá Mesquita entende que o regime do art. 18º da Lei n.º 109/2009 "intersecta-se com dois problemas de articulação legal: os dispositivos sobre escutas telefónicas do Código de Processo Penal e a previsão do art. 9º da Lei n.º 32/2008, de 17 de Julho sobre a transmissão de dados."[102]

No que concerne à articulação do art. 189º do CPP com o art. 18º da Lei n.º 109/2009, este autor defende ainda que, sendo realidades distintas, não podemos articulá-las. Tal justifica a sua crítica ao que designa como a "recusa legislativa" (em prever) "um ponto de referência superador do artefacto telefone"[103]. Paulo Dá Mesquita conclui que não devemos aplicar o art. 18º da Lei n.º 109/2009 quando esteja em causa a interceção e gravação de conversações ou comunicações telefónicas e que a remissão do n.º4 do art. 18º apenas se aplica às normas previstas no CPP que não contrariem a Lei n.º 109/2009.

Mais refere este autor que "(…) com a entrada em vigor da Lei n.º 109/2009, de 15 de Setembro, restou pouco campo prático para a aplicação do artigo 189º, número 1 do Código de Processo Penal"[104], pelo que deve considerar-se o artigo 189º n.º 1 parcialmente revogado – em relação à ingerência nas comunicações armazenadas em suporte digital, por força da regulação mais completa da Lei n.º 109/2009.

Relativamente à articulação legal do art. 9º da Lei n.º 32/2008 com o art. 18º da Lei n.º 109/2009, não nos alongaremos sobre esta matéria, uma vez que já foi objeto de análise

[98] ALBUQUERQUE, *op. cit.*, Anotação 22 ao art. 189º do CPP, p. 549
[99] VERDELHO, 2009, *op. cit.,* p. 746
[100] *Ibid.,* p. 746
[101] NEVES, *op. cit*., p. 350
[102] MESQUITA, *op. cit*, p. 119
[103] *Ibid.*, p. 119
[104] *Ibid.,* pp. 102-104. *Vg*., também, a este respeito, MARQUES, *op. cit*., p.47

no ponto 4.1. Questão diversa é a de saber como articular a Lei n.º32/2008 com o art. 189º do CPP, sobre a qual nos iremos debruçar no ponto seguinte.

4.3. A Lei n.º 32/2008 e o art. 189º do CPP

Existem incongruências várias na articulação da Lei n.º 32/2008 com o art. 189º do CPP.

A este respeito, Lima Cancela defende que "ao manter inalterados os requisitos de acesso e ao consagrar normas gerais no Código de Processo Penal e normas especiais na Lei n.º 32/2008, o legislador tornou este regime especial num regime desnecessário, sem motivo para se denominar como autónomo."[105] Mais conclui o autor que "a criação da Lei nº 32/2008 e nº 109/2009 levam a uma revogação tácita das normas do Código de Processo Penal que regulam a prova digital. Ao serem sobrepostas as leis extravagantes à lei geral, o âmbito de aplicação é restringido, sendo esta última apenas aplicável nas matérias não reguladas. Por essa situação, questionamos a decisão do legislador de não revogação."[106]

De idêntica forma, João Conde Correia entende que o legislador ficou aquém das expetativas, uma vez que optou por remeter " (...) aquilo que constitui hoje o cerne da prova […] para a lei secundária." [107] Assim, entende o autor que as normas gerais deviam estar reguladas no CPP, "reservando a consagração de normas especiais para a Lei n.º 32/2008."[108] Só assim seria possível evitar, em seu entendimento, a duplicação de regimes.

Face ao exposto, também nós somos forçados a concluir que, perante um articulado de diplomas legais que são incoerentes entre si, conducentes a mais dúvidas do que certezas, não se entende a existência de três diplomas que regulam a mesma matéria. Assim, consideramos que é urgente que se proceda a uma uniformização legislativa[109].

[105] CANCELA, *op. cit.*, p. 28
[106] *Ibid.,* p. 28
[107] CORREIA, *op. cit*., p. 54 a 56
[108] *Ibid.*, p. 56-59
[109] A este respeito, *vg*. ainda DIAS, *op. cit.*, p. 20

5. A UTILIZAÇÃO DO CORREIO ELETRÓNICO: CONSIDERAÇÕES ACERCA DAS IMPLICAÇÕES JURÍDICO-CONSTITUCIONAIS

Com o advento das novas tecnologias, surgiram novas formas de comunicar, que vieram "encurtar" a distância entre as pessoas.

Mas, se, por um lado, o progresso da tecnologia facilita a comunicação, por outro, como afirma Dias, "deixa-nos a todos expostos e torna-nos alvos extremamente vulneráveis a ataques perante falhas de segurança e dá vida a "virtual criminal communities e ao "mundo underground"."[110]

Importa, por isso, definir limites no que respeita à ingerência de terceiros em comunicações privadas, de forma a travar "ataques a direitos fundamentais"[111].

Neste capítulo vamos reportar-nos aos direitos fundamentais que são mais suscetíveis de sofrer contrições com a utilização do correio eletrónico como meio de obtenção de prova em processo penal.

5.1.Os direitos implicados

5.1.1. O art. 34º da CRP

A CRP consagra no art. 34.º a inviolabilidade do domicílio e o sigilo da correspondência e de outros meios de comunicação privada.

Com este preceito normativo há uma incontestável vontade do legislador em salvaguardar a privacidade das pessoas, ao considerar o domicílio uma "projeção espacial da pessoa e a correspondência como extensão da própria pessoa"[112], nas palavras de Gomes Canotilho e Vital Moreira.

Chegados aqui, importa fazer um parêntesis para definir o que está efetivamente abrangido pelo direito ao "*sigilo da correspondência e de outros meios de comunicação privada*".

---

[110] DIAS, *op. cit.*, p. 65

[111] COSTA, José Francisco de Faria, *op. cit.*, p. 65. *Vg. ainda* MARQUES, Garcia e MARTINS, Lourenço, *op. cit.,* 2006, p. 425

[112]CANOTILHO, J.J. Gomes e MOREIRA, Vital – *Constituição da República Portuguesa Anotada*, 1993. Autor da anotação não identificado, Anotação I ao art. 34º, p. 212.

Segundo Gomes Canotilho e Vital Moreira, "o conteúdo do direito ao sigilo da correspondência e de outros meios de comunicação privada abrange toda a espécie de correspondência de pessoa a pessoa (cartas postais, impressos), cobrindo mesmo as hipóteses de encomendas que não contem qualquer comunicação escrita, e todas as telecomunicações (telefone, telegrama, telefax, etc)."[113]

Não nos revemos nesta posição, por entendermos que a proteção da esfera privada do sigilo da correspondência só se pode concretizar quando a correspondência circula de forma fechada.

Acompanhamos de perto a posição defendida por Germano Marques da Silva e Fernando Sá, que advogam não ser correspondência fechada "um simples postal, ainda que contendo informação da esfera privada"[114] ou "o e-mail profissional, quando suscetível de ser conhecido ou manipulado pela entidade empregadora."[115] Tal como, também as "muitas das comunicações realizadas através das chamadas redes sociais não têm tutela constitucional porque não oferecem as condições de inviolabilidade necessárias para tal, ou em virtude de serem facilmente acessíveis a uma panóplia de utilizadores que não apenas os destinatários dessa informação."[116] Contrariamente, referem estes autores que "o fax, o e-mail, telefone e videotelefone partilham, em regra, da garantia constitucional do sigilo."[117]

No que concerne ao âmbito da garantia do sigilo da correspondência e das informações transmitidas pelos restantes meios de comunicação, referem estes autores que "A garantia do sigilo abrange não apenas o conteúdo da correspondência, mas o "tráfego" como tal (espécie, hora, duração, intensidade de utilização)."[118] Igualmente, entende Ana Claro Oubiña que "o âmbito de tutela do direito ao sigilo das telecomunicações abrange, em princípio, não só o conteúdo da comunicação, mas também os dados de tráfego e os dados de localização."[119]

---

[113] CANOTILHO e MOREIRA, *op. cit.*, Autor da anotação não identificado, Anotação IV ao art. 34º, p. 213

[114] SILVA, Germano Marques da e SÁ, Fernando, Anotação XIII ao art. 34º - MIRANDA, Jorge e MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Vol. I, 2ª Edição Revista, 2017, p. 560

[115] *Ibid*, ,p. 560. A este respeito, v*g.* ainda Acórdão do Tribunal Constitucional nº 241/02, de 29 de Maio

[116] *Ibid.,* p. 560

[117] *Ibid.*, p. 560.

[118] *Ibid.*, p. 560.

[119] OUBIÑA, Ana Mercedes da Silva Claro - As telecomunicações, a vida privada e o direito penal, 2009, p. 16

Se dúvidas parecem não existir quanto à tutela do direito do sigilo das telecomunicações no que respeita aos dados de tráfego e aos dados de localização, questão mais controversa prende-se com os dados de base[120]. Cristina Máximo dos Santos entende que não há nenhum interesse público que justifique a proteção própria do sigilo de telecomunicações (estando abrangidos apenas por relação de confidencialidade estabelecida numa base contratual entre utente e operadora de telecomunicação). Neste sentido, esta mesma autora vem dizer que não deve confundir-se o sigilo das telecomunicações com a confidencialidade das mesmas[121]. Contrariamente, Ana Claro Oubiña entende que os dados de base devem beneficiar da proteção do direito ao sigilo das telecomunicações, exceto nos casos em que os utentes optem pela "não confidencialidade relativamente ao numero de determinado telemóvel e ao nome e/ou residência do seu titular (…)."[122]

Sendo o direito à inviolabilidade do domicílio e da correspondência um direito fundamental, o âmbito de restrição deste preceito terá, por isso, de ser bastante limitado. Nesta senda, o legislador, no n.º 4 do art. 34º da CRP, optou por vedar às autoridades públicas e privadas o acesso à correspondência, telecomunicações e outros meios de comunicações. Segundo Gomes Canotilho e Vital Moreira esta proibição de toda e qualquer ingerência de entidades públicas e privadas "é mais vasta, envolvendo nomeadamente a liberdade de envio e de receção de correspondência, a proibição de retenção ou de apreensão, bem como de interferência (telefónica, etc)"[123], posição que acompanhamos. A este respeito, convém ainda não esquecer o art. 18º da CRP que, na opinião de Canotilho e Moreira, funciona como "limite absoluto à discricionariedade legislativa neste campo"[124]. Ou seja, só poderá existir ingerência nas telecomunicações se estas estiverem sujeitas ao princípio da necessidade, adequação, proporcionalidade e determinabilidade (art. 18º da CRP).

---

[120] De forma a melhor entender a diferenças entre as três espécies de tipologias de dados *Vg.* o parecer do Conselho Consultivo do MP, nº 21/2000 de 16/6, disponível em www.dgsi.pt e Acórdão do Tribunal da Relação de Évora, de 26 de Julho de 2007 (Proc. nº 843/07-1)

[121] SANTOS, Cristina Máximo dos – As novas tecnologias da informação e o sigilo das telecomunicações. 2004, p. 95 e ss.

[122] OUBIÑA, *op. cit.*, p. 16

[123]CANOTILHO e MOREIRA, *op. cit.*, Autor da anotação não identificado, Anotação VI ao artigo 34º, p. 214

[124] CANOTILHO e MOREIRA, *op. cit.*, Autor da anotação não identificado, Anotação II ao artigo 34º, p. 213

5.1.2. O art. 35º da CRP

Relacionado com o sigilo da correspondência e de outros meios de comunicação privada (art. 34º da CRP) está o direito à autodeterminação informativa, consagrado no art. 35º da CRP, com a epígrafe "Utilização da Informática".

Germano Marques da Silva e Fernando Sá entendem que este direito "tem por finalidade evitar intromissões abusivas na vida privada das pessoas através da recolha e tratamento de dados pessoais informatizados, muito embora a sua materialidade vá para além da tutela da esfera íntima de vida de cada um."[125]

Em idêntico sentido, Catarina Sarmento e Castro refere que este direito é muito mais do que um "direito de garantia do direito à reserva da vida privada, ou um direito que resguarda o cidadão das intromissões não autorizadas de terceiros nas informações que lhe respeitam, num sentido de direito de defesa."[126] Entende esta autora que o direito à autodeterminação informativa deve ser um direito que "permite ao individuo negar informação pessoal ou opor-se à sua recolha e difusão, impondo-se face às agressões do Estado e de terceiros, os quais deverão abster-se de proceder a tratamentos dos seus dados pessoais."[127]

Seguimos o parecer dos autores supra referidos no sentido em que entendemos que o direito à autodeterminação informativa não se deve limitar aos factos da esfera privada de cada pessoa. Este direito constitucionalmente consagrado deve ser lido como uma garantia da segurança dos dados pessoais (de natureza sensível) de um determinado titular que controla a informação que sobre si é fornecida, bem como os termos do seu tratamento por terceiros.

5.1.3. O art. 26º da CRP

O direito à reserva sobre a intimidade da vida privada encontra-se consagrado no art. 26º da CRP.

---

[125] SILVA, Germano Marques da e SÁ, Fernando, Anotação V ao artigo 35º - MIRANDA e MEDEIROS, *op. cit*., p. 569

[126] CASTRO, Catarina Sarmento e – *Direito da Informática, Privacidade e Dados Pessoais,* 2005, p.27

[127] *Ibid,* p. 27. Relativamente à definição de "dados pessoais", *vg*. ainda o art. 3º da Lei de Proteção dos Dados Pessoais e art. 4º º1 do Regulamento Geral da Proteção de Dados, este último que entrou em vigor no ordenamento jurídico português no passado dia vinte e cinco de maio do corrente ano

Consagra esta norma constitucional, no seu n.º1, que "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação".

No âmbito deste trabalho vamos apenas abordar, neste contexto, a questão do direito à reserva da intimidade da vida privada, do qual derivam os postulados da garantia do direito à inviolabilidade do domicílio e o sigilo da correspondência e de outros meios de comunicação privada (art. 34º da CRP) e o direito à autodeterminação informativa (art. 35º da CRP).

No que concerne à reserva da intimidade da vida privada, partilhamos a opinião de Ana Luísa Pinto quando afirma que "O direito à reserva da intimidade da vida privada tutela, essencialmente, o interesse de cada pessoa em controlar a informação sobre a sua vida privada, impedindo que terceiros possam, sem o seu acordo, tomar conhecimento ou divulgar essa informação."[128]

Sobre esta questão, refere o Acórdão n.º 128/92 de 24 de Julho, do Tribunal Constitucional que "O homem, sendo embora um ser social, não é, porém, todo ele parte da sociedade civil. Justamente porque é pessoa, o homem tem um âmbito pessoal em que não têm entrada nem o Estado, nem a sociedade, um âmbito regulado pela consciência e pelo juízo de cada um. Este âmbito privado (intimo, próprio) não é em si mesmo objeto de regulamentação por parte do Estado, nem de ingerências sociais. É um âmbito de liberdade, de intimidade ou de não publicidade."[129]

Daqui podemos retirar que tanto a doutrina, como a jurisprudência têm procurado impedir o acesso a terceiros à informação do foro privado de determinada pessoa.

Na tentativa de reforçar a proteção constitucional do sigilo das telecomunicações elencado nos números 2 e 3 do artigo 18.º da CRP, surge o nº 8 do art. 32º da CRP que comina *"com a nulidade as provas obtidas mediante a abusiva intromissão na vida privada ou nas telecomunicações."*

[128] PINTO, Ana Luísa *apud* NEVES, *op. cit.*, p. 34
[129] Acórdão n.º 128/92 de 24 de Julho de 1992, do Tribunal Constitucional

É precisamente a este propósito que se levantam as principais dificuldades já que, como bem refere Rita Castanheira Neves "há uma "tensão dialética" entre o princípio da reserva da intimidade da vida privada e o princípio da descoberta da verdade material."[130]

Neste âmbito, surge como questão central saber em que casos são admitidas as ingerências nas comunicações por parte do Estado (à luz do n.º 8 do art. 32º e n.º 4 do art. 34º da CRP).

Em resposta a esta questão de grande complexidade, consideramos que as barreiras de permissão devem ser restritas -em nome da salvaguarda dos direitos, liberdades e garantias conquistadas- pois só assim podemos separar as ingerências que são invioláveis, daquelas que podem ser utilizadas como meio de obtenção de prova em processo penal.

Concordamos com Germano Marques da Silva[131] na parte em que defende que, existindo colisão de direitos, devemos sempre escolher o meio que seja menos oneroso (principio da proporcionalidade). Defende este autor que, não sendo a verdade processual absoluta, os meios para a descoberta da verdade não podem ser usados a qualquer custo, comprometendo os direitos fundamentais. No limite, tem de haver situações de cedência que se circunscrevam ao indispensável. Neste sentido, entende o autor que "entre o interesse público na perseguição penal e o interesse publico também da tutela de determinados interesses, a ordem jurídica opta por uns ou por outros, conforme considere que devem prevalecer, pois a perseguição penal não é necessariamente o interesse predominante da vida em sociedade."[132]

Em perspetiva idêntica, afirma Benjamim da Silva Rodrigues que "qualquer ingerência em dados de caráter pessoal, armazenados em ficheiros automatizados de dados pessoais, sejam elas informatizadas ou não, implicam uma lesão num direito fundamental que tem de ser sopesado com um correspetivo interesse ou direito prevalente ou, nalguns casos, por valores mais elevados inerentes às sociedades democráticas (defesa da integridade nacional, segurança pública, defesa nacional, etc)."[133]

Neste âmbito, o art. 8º da Convenção Europeia dos Direitos do Homem surge como normativo imprescindível em matéria de dados pessoais. Segundo este artigo, apenas "são admitidas ingerências das autoridades públicas, ao nível da vida privada e familiar,

[130] NEVES, *op. cit*, p.30
[131] SILVA, Germano Marques da - *Curso de Processo Penal*, Vol. II, 2010
[132] *Ibid.* p. 103
[133] RODRIGUES, *op. cit.,* 2008, pp. 259 e 260

domicilio e correspondência, quando ela estiver prevista na lei (principio da legalidade) e constituir uma providência que, numa sociedade democrática (principio da democraticidade) seja necessária (principio da necessidade e principio da proporcionalidade) para a defesa da segurança nacional e pública, para o bem-estar económico do país, a defesa da ordem, a prevenção das infrações penais, a proteção da saúde ou da moral, bem como da proteção dos direitos e liberdades de terceiros."

Todavia, e uma vez que há a possibilidade de existirem outras causas de justificação da ingerência ou restrição de direitos, terá de ser feita uma análise casuística, tendo presente o princípio estrito da proporcionalidade e da necessidade de tutela penal na ponderação dos direitos em conflito.

6. ALGUMAS REFLEXÕES SOBRE A PROVA DIGITAL E O CORREIO ELETRÓNICO- PERSPETIVAS DE FUTURO.

O desenvolvimento tecnológico que se fez sentir particularmente em finais do século passado levou a uma profunda modificação social, laboral e económica.

Um dos maiores problemas com que nos deparamos diz respeito às intromissões na esfera privacidade, a que os cidadãos "assistem de forma apática e obediente"[134].

Em virtude da facilidade de acesso ao mundo virtual, podemos hoje ter acesso na rede a diversos tipos de informações sobre determinada pessoa. Como referem Manuel Lopes Rocha e Mário Macedo, seja "através de transações bancárias, escolha de programas audiovisuais, envio de mensagens, vigilância à distância do domicílio, utilização de jogos-video, CD de música por encomenda, enfim, aquisição de bens e serviços. Através de todas estas utilizações, cada um de nós vai gerando cada vez mais dados e mais precisos sobre os nossos hábitos de consumo e de vida."[135]

Ao subscreverem um serviço, as pessoas disponibilizam os seus dados a empresas que vendem as suas informações, sem que o utilizador saiba verdadeiramente como são recolhidos e como vão ser tratados os seus dados, levando a um "verdadeiro desapossamento da pessoa."[136]

Esta nova vaga de fluxos comunicacionais digitais levanta sérios problemas a que o direito penal e direito processual penal têm procurado dar resposta.

6.1. As especificidades da prova digital

Não existe uma definição consensual para a "prova digital".

A prova digital é descrita por Benjamim da Silva Rodrigues como "qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de

---

[134] *Ibid*, p. 436

[135] ROCHA, Manuel Lopes e MACEDO, Mário - *Direito no Ciberespaço*, 1996, p. 101.
Neste quadro, é ainda de salientar a importância de aplicações como o *Facebook*, *Tweet*er, *Instagram*, *Skype*, *WhatsApp*

[136] RODRIGUES, *op. cit*, 2008, p. 436

comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital."[137]

Por outro lado, Armando Dias Ramos entende que prova digital é "a informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) de ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta."[138]

6.2. Dificuldades suscitadas pela sua natureza

Ao contrário do que acontece com as provas documentais, a prova digital não é suscetível de apreensão material e, na medida em que a sua utilização pode ser feita em qualquer local do mundo, "sem qualquer contato físico com os sistemas informáticos ou dados atingidos"[139], por qualquer pessoa com acesso a um computador ligado à Internet, há a possibilidade desta ser a todo o momento alterada.

A prova digital possui caraterísticas que a tornam singular, uma vez que, como declara Benjamim da Silva Rodrigues, é "fragmentária, dispersa, frágil, volátil, alterável, instável, apagável e manipulável, invisível e espacialmente dispersa"[140], sendo, por isso, extremamente difícil preservar, analisar e garantir a fiabilidade desta prova a apresentar em julgamento[141].

A adensar o problema está o facto de a legislação portuguesa não prever instrumentos de investigação específicos para a prova digital, o que faz com que a maior parte dos inquéritos em investigação relativos a criminalidade informática continuem a ter como desfecho o arquivamento por inexistência de indícios suficientes da prática do crime[142].

---

[137] RODRIGUES, Benjamim da Silva - *Da Prova Penal IV, Da Prova Eletrónico-Digital e da Criminalidade Informático-Digital,* 2011, p. 722
[138] RAMOS, *op. cit.*, p. 86
[139] MILITÃO, *op. cit.*, p. 261
[140] RODRIGUES, *op. cit.*, 2011, p.29
[141] Neste sentido, *vg.* MILITÃO, *op. cit*, p. 261
[142] Neste sentido, *vg.* LOPES, José Mouraz e CABREIRO, Carlos Antão - A Emergência da Prova Digital na Investigação da Criminalidade Informática, 2006, p. 72

Como bem denota Rita Coelho dos Santos, "a criminalidade informática faz reavivar a problemática da prova"[143], pois implica meios de obtenção de prova, com caraterísticas diferentes dos meios tradicionais.

Face ao exposto, é nossa convicção que o ordenamento jurídico português necessita de uma alteração profunda em matéria de direito probatório. Só com novos e rigorosos critérios será possível garantir a recolha e a conservação da prova digital durante mais tempo e, simultaneamente, inspirar confiança nos que dela fazem uso.

6.3. As perspetivas de futuro: propostas a considerar

Encetámos o estudo desta temática cientes que existem várias dificuldades suscitadas pela natureza da prova digital, designadamente a dificuldade da sua recolha e conservação, e a possibilidade de esta ser facilmente manipulável.

Não obstante, pensamos que é possível apresentar algumas sugestões para obviar os problemas detetados.

Como pressuposto, entendemos que é importante que exista um conhecimento dos riscos inerentes ao mundo virtual por parte das pessoas, para que, de forma mais consciente e informada, sejam tomadas medidas eficazes para o seu combate.

Assim, entendemos que a prevenção através da sensibilização das pessoas para os perigos do mundo cibernético é extremamente importante[144] para travar o avanço das novas tecnologias da informação e da comunicação, que tem levantado, como vimos, sérios problemas sociais.

Mas, a par da prevenção existem outras soluções a que importa atender. Entre elas, destacamos a possibilidade de cooperação entre entidades policiais e judiciárias em matéria de prova digital. Na esteira de Renato Lopes Militão, entendemos que só é possível existir uma estreita cooperação internacional se as entidades competentes forem

[143] SANTOS, Rita Coelho dos - *O tratamento jurídico-penal da transferência da manipulação ilícita dos sistemas informáticos*, 2005, p. 53

[144]Vera Elisa Dias é de opinião que "a prevenção será alcançada com informação, sensibilização e preparação, através de seminários, campanhas visadas a um público-alvo comum ou específico, alertando para os riscos e perigos do mundo cibernético e os meios e proteção e responsabilidade de utilização." (DIAS, *op. cit.*, p. 77). A este respeito, *vg*., ainda, RODRIGUES, *op. cit.,* 2008, p. 238

"dotadas de recursos humanos e meios técnicos e tecnológicos capazes de dar resposta"[145] – as chamadas unidades especializadas para o efeito.

Como já foi referido anteriormente, o pulsar das tecnologias trouxe novos desafios ao direito processual penal, que terá de atualizar-se de forma a acompanhar o desenvolvimento das Tecnologias da Informação e da Comunicação (doravante TIC). Neste contexto, e à luz da fragilidade da prova digital, que continua a levantar vários problemas ao nível da verificação da identidade da pessoa que praticou determinada conduta, a certificação da assinatura digital parece ser uma alternativa cada vez mais viável, na medida em que permite a cifragem das mensagens enviadas por correio eletrónico, com a confirmação da autenticidade da origem e integridade do texto de determinado documento, levando a que se "presuma que o indivíduo "A" foi o autor da conduta investigada"[146]. Todavia, ao direito penal não podem bastar meras suposições. Assim, não existindo uma forma de validar a autoria dos documentos eletrónicos e não havendo como garantir que qualquer documento foi alterado, as dúvidas persistem.

Com o intento de melhorar a segurança dos utilizadores no ambiente digital, a criptografia pode constituir um mecanismo de proteção da almejada privacidade.

Como bem refere Joel Timóteo Ramos Pereira, "os algoritmos de criptografia vão permitir aos utilizadores de um sistema codificar mensagens, ficheiros, e outra informação digital de uma forma tal, que só o autor e o destinatário desejado das mensagens a possam decifrar"[147], o que levará a uma maior proteção dos dados dos particulares, reduzindo-se, assim, a possibilidade de transmissão de dados pessoais informatizados.

Outra eventual solução é apontada por Armando Dias Ramos que, perspetivando que no futuro a comunicação seja feita por mensagens faladas (videoconferências, *stream* de vídeos e mensagens eletrónicas de áudio), considera que os servidores e serviços têm, também eles, de se adaptar às novas exigências dos utilizadores e passar a estar acessíveis através da *cloud*, em qualquer ponto do mundo[148].

[145] MILITÃO, *op. cit.*, p. 262
[146] *Ibid*, p. 264
[147] PEREIRA, Joel Timóteo Ramos - *Direito da Internet e Comércio Eletrónic*o, 2001, p. 40
[148] RAMOS, *op. cit.*, pp. 107-111

Este autor propõe ainda a criação de um Código de Direito da Informática, "onde numa só compilação se reúna toda a legislação a nível penal e a nível processual penal."[149]

Não nos revemos nesta posição por considerarmos que os meios disponibilizados pelo Direito Penal são suficientes[150]. Assim, e como bem refere Manuel Monteiro Guedes Valente, entendemos que não devem ser criados direitos penais especiais sob pena de desvirtuar o direito penal e direito processual penal[151].

De entre as soluções referidas parece-nos que, a assinatura digital pode ser uma solução a considerar, na medida em que garante a integridade dos dados apreendidos relativamente a alterações posteriores, sendo também a solução que - comparativamente com as restantes aqui apresentadas - é mais eficiente e economicamente sustentável.

[149] RAMOS, *op. cit.,* p. 108

[150]No mesmo sentido, José Francisco de Faria Costa entende que não devemos "diabolizar a informática". Assim, conclui este autor que, "apesar das suas particularidades e tratando-se de um canal comunicacional amplo e complexo, não se verifica a "sustentabilidade científica para autonomizar um direito penal da informática" COSTA, José Francisco de Faria *apud* RAMOS*, op, cit.* p.111

[151] Segundo este autor, é de criticar "a opção legislativa dos últimos tempos com a criação de Direitos penais especiais- económico, bancário, tributário, ambiental, do crime organizado, do terrorismo, (etc.) – e, por consequência, de Direitos processuais penais especiais integrantes do próprio diploma material, desintegrados do Código de Processo Penal, como se fossem tão especiais aos quais não se aplicam os mesmos princípios axiológico-constitucionais do Direito penal material e processual de justiça. É um outro Direito para outros atores judiciários e para outros delinquentes e outras vítimas (invisíveis), violando-se o núcleo central da legalidade: a igualdade." (VALENTE, Manuel Monteiro Guedes Valente - *Processo Penal*- Tomo I, 2010, p. 19).

7. CONSIDERAÇÕES FINAIS

Com o advento das novas tecnologias, impulsionadas pela Internet, surgiram novos tipos de crimes e novos métodos de investigação que suscitam questões a nível do direito processual penal.

Não obstante as significativas alterações levadas a cabo pela reforma do CPP, em dois mil e sete, consideramos que o legislador, ao tentar adaptar o regime das escutas telefónicas a outros meios de comunicação (art. 189º do CPP), misturou duas realidades distintas - a interceção e registo de comunicações ou conversas realizadas (em tempo real) através de meio técnico diferente do telefone, e as comunicações eletrónicas que se encontrem armazenadas em suporte digital – gerando ainda mais interrogações.

Mais entendemos que, com a atual redação do art. 189º do CPP, o legislador confunde a palavra falada e escrita. Na nossa ótica, sendo distinto o grau de intromissão das comunicações faladas e escritas distinto, o regime das escutas apenas deveria incidir sobre os processos de comunicação oral.

No que concerne à interceção do correio eletrónico em tempo real, sufragamos a posição de Rita Castanheira Neves e Costa Andrade no sentido de não podermos aplicar o art. 189º do CPP. Após a leitura do correio eletrónico pelo seu destinatário, a sua função está cumprida. Já não estamos perante uma comunicação e por isso, o correio eletrónico não pode ser intercetado. Sendo um mero "documento" armazenado no computador, devemos subsumi-lo ao regime das buscas e apreensões. O que significa que, de forma a apreender suportes digitais resultantes de comunicações eletrónicas, teremos de apreender o suporte físico a elas inerente, neste caso, o computador. Alguns autores, entre eles, Rita Castanheira Neves, entendem que podem ainda ser apreendidas cópias integrais ou parciais dos conteúdos presentes nos computadores para outros suportes, como CDs, DVDs e *pens*.

Em virtude da grave ingerência aos direitos fundamentais que o acesso a dados sensíveis constitui, a doutrina tem vindo a refletir acerca da busca *online* enquanto meio de prova em processo penal.

No que se refere à questão da "interceção das comunicações entre presentes", também ela consagrada no art. 189º do CPP, é nossa convicção que sendo as telecomunicações e as comunicações entre presentes realidades distintas, não deviam ter

sido reconduzidas ao mesmo preceito. Atente à danosidade social que representam, as segundas deveriam gozar de um regime autónomo, mais exigente e seletivo.

Todavia, o estudo do correio eletrónico enquanto meio de prova em processo penal não se resume ao vertido no CPP. Nesta perspetiva, analisámos outros diplomas (internacionais e nacionais), através dos quais foi possível analisar as semelhanças e contrastes em matéria de ingerências em comunicações eletrónicas, o que confere neste momento algum alento para expor algumas conclusões.

No que respeita à Lei n.º 32/2008, aplaudimos a preocupação do legislador em estabelecer os requisitos de admissibilidade e as formalidades no acesso, conservação e transmissão dos dados de tráfego e localização, bem como dos dados relevantes para a identificação do utilizador, garantindo a investigação e repressão de crimes graves de forma mais célere. Contudo, a transposição da Diretiva n.º 2006/24/CE, nestes moldes, acabou por ser um verdadeiro desastre uma vez que o legislador veio duplicar desnecessariamente os regimes em matéria de prova, situação que poderia ter sido evitada se esta lei apenas regulasse questões técnicas respeitantes à conservação dos dados.

Com a ratificação portuguesa à Convenção sobre o Cibercrime e a transposição da Decisão Quadro n.º 2005/222/JAI, o legislador criou a Lei n.º109/2009, na qual aglutinou normas de direito penal material, processual e normas de cooperação internacional.

Levantam-se vários problemas a respeito da harmonização desta Lei com o consagrado na Lei n.º 32/2008. Sendo as disposições nelas constantes díspares, entendem alguns autores que devemos aplicar o princípio da "*lex posteriori derogat lex priori*", ou seja, a Lei n.º 109/2009 revogaria a Lei n.º 32/2008. Contudo, a maioria da doutrina e jurisprudência conclui que o objetivo do legislador seria a articulação de ambas as leis (n.º 2 do art. 11º da Lei n.º 109/2009), o que se tem revelado extremamente difícil.

Apesar da tentativa de harmonização do disposto no art. 17º da Lei n.º 109/2009 e do art. 189º do CPP, consideramos que a Lei do Cibercrime, ao passar a regular a matéria das ingerências nas comunicações eletrónicas, deixou um campo de aplicação muito escasso para o CPP. O legislador deveria ter consagrado o regime de obtenção de prova num único capítulo do CPP, adequado às exigências instituídas pelas novas tecnologias.

Como é consabido, o advento das novas tecnologias da informação e da comunicação, ao mesmo tempo que facilitou a comunicação entre as pessoas, potenciou também riscos de violação da privacidade.

Como forma de salvaguardar os direitos, liberdades e garantias conquistadas, foram consagrados constitucionalmente vários preceitos a este respeito: o direito à inviolabilidade do domicílio e o sigilo da correspondência e de outros meios de comunicação privada (art. 34º da CRP), o direito à autodeterminação informativa (art. 35º da CRP) e o direito à reserva da intimidade da vida privada (art. 26º da CRP).

Contudo, subsistem ainda algumas dúvidas na aplicação destes normativos constitucionais: como separar as ingerências que são invioláveis, daquelas que podem ser utilizadas como meio de prova em tribunal? De forma a poder responder a esta questão, importa, antes de mais, sobrepesar as especificidades técnicas em causa e, posteriormente aferir do respetivo potencial de lesão dos valores implicados, escolhendo o meio menos oneroso, em respeito pelo princípio da proporcionalidade e da necessidade da tutela penal.

De facto, têm sido feitos progressos significativos em matéria de prova digital nos últimos anos. Todavia, na nossa ótica, há ainda um longo caminho a percorrer.

Numa perspetiva de futuro, é importante que se sanem de vez as discrepâncias dos dispares diplomas respeitantes à prova digital, levando a cabo uma reforma profunda do atual CPP, mas, isto não basta. Importa ainda mudar as mentalidades dos utilizadores da Internet, alertando-os para os riscos da sua imprudente utilização.

Cabe nesta sede referir que, a par da prevenção existem outras formas de travar o avanço desenfreado das TIC, entre elas, destacamos a criptografia e a assinatura digital, que, garantindo a integridade dos dados apreendidos relativamente a alterações posteriores, constituem cada vez mais uma opção a considerar.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, Paulo Pinto de - *Comentário ao Código de Processo Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*. 2ª ed. atualizada. Lisboa: Universidade Católica Editora, 2008.

ANDRADE, Manuel da Costa - *Sobre as Proibições de Prova em Processo Penal*. Coimbra: Coimbra Editora, 1992.

_____- *"Bruscamente no verão passado", a reforma do Código do Processo Penal - Observações crítica sobre uma Lei que podia e devia ter sido diferente*. Coimbra: Coimbra Editora, 2009.

BRAVO, Rogério - Da não equiparação do correio eletrónico ao correio tradicional de correspondência por carta. *Revista de Polícia e Justiça.* III Série, Janeiro – Junho, nº 7, (2006), pp. 207-216.

CANCELA, Alberto Gil Lima - *A prova digital*: os *meios de obtenção de prova na Lei do Cibercrime.* Coimbra: Faculdade de Direito da Universidade de Coimbra, 2016. Dissertação de Mestrado, Especialização em Ciências Jurídico-Forenses.

CANOTILHO, J. J. Gomes e MOREIRA, Vital - *Constituição da República Portuguesa Anotada.* 3.ª edição revista. Coimbra: Coimbra Editora, 1993.

CARDOSO, Vanessa Chagas - *Telecomunicações e prova em processo penal: das escutas telefónicas à intromissão nas comunicações electrónicas.* Coimbra: Faculdade de Direito da Universidade de Coimbra, Junho de 2014. Dissertação de Mestrado, Especialização em Ciências Jurídico-Forenses.

CASTRO, Catarina Sarmento e - *Direito da informática, privacidade e dados pessoais.* Coimbra: Edições Almedina, 2005.

CORREIA, João Conde - Prova Digital: as leis que temos e a lei que devíamos ter. *Revista do Ministério Público*. 139: Julho- Setembro (2014), pp. 29-59.

COSTA, Catarina Rodrigues Santos - *As proibições de prova e a prova digital – aproximação aos lugares-comuns de um instituto clássico em face de uma nova realidade*. Braga: Faculdade de Direito da Universidade do Minho, Outubro de 2017.

Dissertação de Mestrado em Direito Judiciário (direitos processuais e organização judiciária).

COSTA, José Francisco de Faria – *Direito Penal da Comunicação : alguns escritos*. Coimbra: Coimbra Editora, 1998.

DIAS, Vera Marques - A problemática da investigação do Cibercrime. *Data Venia Revista Jurídica Digital*, n.º1, Julho-Dezembro (2012), pp. 64-87. Disponível em http://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063-088.pdf.

GONÇALVES, Pedro Costa - *Direito das Telecomunicações*. Coimbra: Edições Almedina, 1999.

LEITE, André Lamas - Entre Péricles e Sísifo: o novo regime legal das escutas telefónicas. *Revista Portuguesa de Ciência Criminal*, Ano 17, n.º 4, Outubro- Dezembro (2007), pp. 654-668.

LOPES, José Mouraz - *Garantia Judiciária no Processo Penal: do Juíz e da Instrução*. Coimbra: Coimbra Editora, 2000.

LOPES, José Mouraz e CABREIRO, Carlos Antão - A Emergência da Prova Digital na Investigação da Criminalidade Informática. *Sub Judice - Justiça e Sociedade*, n.º 35, Abril-Junho (2006), pp. 71-79.

MARQUES, Garcia e MARTINS, Lourenço - *Direito da Informática*. 2.ª ed. Refundida e Atualizada. Coimbra: Editora Almedina, 2006.

MARQUES, Maria Joana Xara-Brasil - *Os meios de obtenção de Prova na Lei do Cibercrime e o seu confronto com o Código de Processo Penal*. Lisboa: Universidade Católica Portuguesa - Escola de Direito de Lisboa, Julho de 2014. Dissertação de Mestrado Forense.

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

MILITÃO, Renato Lopes - A Propósito da Prova Digital. *Revista da Ordem dos Advogados Portugueses*, 72, n.º 1 (2012), pp. 247-285.

MIRANDA, Jorge e MEDEIROS, Rui - *Constituição Portuguesa Anotada*. Vol. I. 2ª edição revista. Lisboa: Universidade Católica, Fevereiro de 2017.

NEVES, Rita Castanheira - *As ingerências nas Comunicações Eletrónicas em Processo Penal- natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*. Coimbra: Coimbra Editora, 2011.

OLIVEIRA, Margarida Viana Guarda de - *Proteção de Dados Pessoais nas Comunicações Eletrónicas: o papel da CNPD e da* ANACOM. Lisboa: Universidade Católica Portuguesa, Faculdade de Direito, Outubro de 2015. Dissertação de Mestrado em Direito Administrativo.

OUBIÑA, Ana Mercedes da Silva Claro - As telecomunicações, a vida privada e o direito penal. In: ANDRADE, Manuel da Costa e NEVES, Rita Castanheira, org. *Direito Penal hoje – Novos desafios e novas respostas*. Coimbra: Coimbra Editora, Agosto de 2009.

PEREIRA, Joel Timóteo Ramos - *Direito da Internet e Comércio Eletrónico*. Lisboa: Sociedade Editora Quid Juris?, 2001.

PINTO, Ana Luísa - Aspetos Problemáticos do regime das buscas domiciliárias. *Revista Portuguesa de Ciência Criminal*. Ano 15, n.º 3, Julho-Setembro (2005), pp. 415-417.

RAMOS, Armando Dias - *A prova digital em Processo Penal: o correio eletrónico*. Lisboa: Chiado Editora, Novembro de 2014.

ROCHA, Manuel Lopes e MACEDO, Mário - *Direito no Ciberespaço – seguido de um Glossário de Termos e Abreviaturas*. Lisboa: Edições Cosmos, 1996.

RODRIGUES, Benjamim Silva - *Da Prova Penal — Tomo IV — Da Prova – Electrónico - Digital e da Criminalidade Informático-Digital*. Lisboa: Rei dos Livros, 2011.

_____- *Das Escutas Telefónicas - Tomo I : a monitorização dos fluxos informacionais e comunicacionais: contributo para a superação do "paradigma da ponderação constitucional e legalmente codificado" em matéria de escutas telefónicas*. Coimbra: Coimbra Editora, 2008.

ROMEO CASABONA, Carlos Maria - La protección penal de los mensajes de correo eletrónico y de otras comunicaciones de caráter personal a través de internet.

Derecho y Conocimiento. vol.2, (2004) pp. 123-149, disponível em https://www.unifr.ch/ddp1/derechopenal/obrasportales/op_20080612_17.pdf

SANTOS, Rita Coelho dos - *O tratamento jurídico-penal da transferência da manipulação ilícita dos sistemas informáticos*. Stvdia Ivridica 82, Coimbra: Coimbra Editora, 2005.

SANTOS, Cristina Máximo dos - As novas tecnologias da informação e o sigilo das telecomunicações. *Revista do Ministério Público*, Ano 25, n.º 99, Julho-Setembro (2004), pp. 89-116.

SILVA, Germano Marques da - *Curso de Processo Penal*. Vol. II, 5.ªed., Lisboa: Verbo, 2010.

SOUSA, Susana Aires de - Agent Provocateur e meios enganosos de prova. Algumas reflexões. In: ANDRADE, Manuel da Costa; COSTA, José de Faria; RODRIGUES, Anabela Miranda; ANTUNES, Maria João (Orgs.). *Liber Discipulorum para Jorge de Figueiredo Dias*. Coimbra: Coimbra Editora, 2003.

VALENTE, Manuel Monteiro Guedes - *Processo Penal* - Tomo I. 3.ª ed. Coimbra: Almedina, 2010.

VEIGA, Armando e RODRIGUES, Benjamim Silva - *Escutas Telefónicas. Rumo à Monitorização dos Fluxos Informacionais e Comunicacionais Digitais.* 2ª ed. Coimbra: Coimbra Editora, 2007.

VERDELHO, Pedro - A obtenção de prova no ambiente digital. *Revista do Ministério Público*, ano 25, nº 99, Julho-Setembro (2004a), pp.117-136.

_____ - Apreensão de correio eletrónico em processo penal. *Revista do Ministério Público*, ano 25, nº100, Outubro-Dezembro (2004b), pp.153-164.

_____ - A nova lei do cibercrime. *Scientia Juridica*, N.º 320 Tomo LVIII, Outubro-Dezembro (2009), pp. 717-749.

JURISPRUDÊNCIA CITADA

- Acórdão do Tribunal de Justiça da União Europeia de 8-04-2014, Proc. n.º C-293/12, consultado em http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=PT#Footnote* .
- Acórdão do Tribunal da Relação de Évora, de 26-06- 2007, Proc. n.º 843/07-1, consultado em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/daa6e41d3c09ff2580257de100574cdd?OpenDocument .
- Acórdão do Tribunal da Relação de Coimbra, de 26-02-2014, Proc. nº 559/12.0GBOBR-A.C1, consultado em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/0e255b331c5eaecd80257c91005ae8bf?OpenDocument
- Acórdão do Tribunal da Relação de Coimbra de 28-01-2009, consultado em CJ, XXXIV, 1, 55;
- Acórdão do Tribunal da Relação de Guimarães, de 12-10-2009, Proc. n.º 1396/08.1PBGMR, consultado em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/4c03909839f95d5f8025767e004f83fe?OpenDocument .
- Acórdão do Tribunal da Relação de Lisboa, de 15-07-2008, Proc. n.º 3453/2008, consultado em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/9182245992c7c5d18025749000503b8c?OpenDocument .
- Acórdão do Tribunal da Relação de Lisboa, de 11-01-2011, Proc. n.º 5412/08.9TDLSB-A.L1-5, consultado em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument .
- Acórdão do Tribunal da Relação do Porto de 27-01-2010, Proc. n.º 896/07.5JAPRT.P1, consultado em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/68fdcdf35dc62b6e802576c40041c799?OpenDocument .

- Acórdão do Tribunal Constitucional n.º 241/02, de 29-05, publicado em Diário da República, II Série, n.º 168, em 23-06, pp. 12 825 a 12 831.
- Acórdão do Tribunal Constitucional n.º 128/92, de 24-07, publicado em Diário da República, II Série, em 24-07-1992, pp. 6807 e ss.

LEGISLAÇÃO CONSULTADA

- Código de Processo Penal.
- Convenção sobre o Cibercrime, de 23 de novembro de 2001.
- Decisão Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005 (relativa a ataques contra sistemas de informação).
- Decreto do Presidente da República nº 92/2009, publicado no Diário da República, Série I, de dezasseis de abril.
- Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006.
- Diretiva nº 2002/58/CE do Parlamento e do Conselho, de 12 de julho de 2002.
- Lei n.º 67/98, de 26 de Outubro (Lei de Proteção dos Dados Pessoais).
- Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime).
- Lei n.º 144/99 de 31/08 (Lei da Cooperação Judiciária Internacional em matéria penal).
- Lei n.º 32/2008, de 17 de Julho (Lei da Conservação de Dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas)
- Parecer do Conselho Consultivo do MP, nº 21/2000 de 16/6.
- Proposta de Lei n.º 289/X/4.ª (Proposta de Lei do Cibercrime)
- Regulamento Geral da Proteção de Dados, de 25 de maio de 2018.
- Resolução da Assembleia da República n.º 88/2009, publicada no Diário da República, Série I, de dia quinze de setembro.