Universidade do Minho
Escola de Direito

Marta Maria Morais da Silva

As comunicações eletrónicas e a investigação criminal (rumo à compreensão do regime de ingerência no seu conteúdo)

outubro de 2017

As comunicações eletrónicas e a investigação criminal (rumo à compreensão do regime de ingerência no seu conteúdo)
Marta Maria Morais da Silva
UMinho | 2017

Universidade do Minho
Escola de Direito

Marta Maria Morais da Silva

As comunicações eletrónicas e a investigação criminal (rumo à compreensão do regime de ingerência no seu conteúdo)

Dissertação de Mestrado
Mestrado em Direito Judiciário

Trabalho efetuado sob a orientação do
Professor Doutor Pedro Freitas

outubro de 2017

DECLARAÇÃO

Nome: Marta Maria Morais da Silva

Endereço eletrónico: martamoraissilva.24@gmail.com Telefone: 917730143

Número do Bilhete de Identidade: 14407856 2 ZY8

Título dissertação: As comunicações eletrónicas e a investigação criminal (rumo à compreensão do regime de ingerência no seu conteúdo)

Orientador: Professor Doutor Pedro Freitas

Ano de conclusão: 2017

Designação do Mestrado: Mestrado em Direito Judiciário

Universidade do Minho, ___/___/_____

Assinatura: _____

À dolorosa luz das grandes lâmpadas elétricas da fábrica
Tenho febre e escrevo.
Escrevo rangendo os dentes, fera para a beleza disto,
Para a beleza disto totalmente desconhecida dos antigos.

Ó rodas, ó engrenagens, r-r-r-r-r-r-r eterno!
Forte espasmo retido dos maquinismos em fúria!
Em fúria fora e dentro de mim,
Por todos os meus nervos dissecados fora,
Por todas as papilas fora de tudo com que eu sinto!
Tenho os lábios secos, ó grandes ruídos modernos,
De vos ouvir demasiadamente de perto,
E arde-me a cabeça de vos querer cantar com um excesso
De expressão de todas as minhas sensações,
Com um excesso contemporâneo de vós, ó máquinas!

Álvaro de Campos

Agradecimentos

Ao longo da elaboração desta Dissertação de Mestrado foram muitas as ocasiões em que necessitei de ajuda. Felizmente, em muitas dessas ocasiões a ajuda chegou – e com ela, a altura de agradecer.

Em primeiro lugar, dirijo o meu agradecimento à pessoa que me orientou na elaboração desta Dissertação, o Professor Doutor Pedro Freitas, pelo tempo que a este trabalho dedicou e por ter partilhado comigo o seu conhecimento: indicou sempre o melhor caminho e contribuiu em muito para que resultado final desta Dissertação fosse o melhor e mais completo possível.

Em segundo lugar, não poderia deixar de agradecer à Faculdade de Direito da Universidade do Porto, por ter sido a instituição que me acolheu e formou no "Direito": a escola de paredes brancas e tetos altos, onde se partilha a sabedoria. Este agradecimento estende-se a todos os professores e funcionários que comigo se cruzaram, e em especial à sua Biblioteca – em cujos meandros se começou a delinear esta tese, e que só com o seu completo recheio seria possível concluir.

Em terceiro lugar, o mais sincero agradecimento à Sociedade Elmiro de Sousa, Rosa Vasconcelos & Associados, a quem dirijo à pessoa da Dra. Rosa Vasconcelos, a minha patrona, por me ter recebido em sua "casa" e ensinado a dar os primeiros passos no mundo da Advocacia, tendo-me sempre encorajado e dado todas as condições para conciliar o estágio e a conclusão desta Dissertação.

Por último, que será sempre em primeiro, uma palavra de gratidão à minha Mãe, Pai, Irmã e Avó (e também ao Chico, claro), que para além desta Dissertação, me acompanham e guiam na vida. Aos meus amigos, pelas horas boas e más, e ao João, por ser o primeiro em tudo, sempre.

Resumo

A investigação criminal depende, muitas vezes, do contributo dos investigados para dar resposta às questões que se levantam com o cometimento de crimes. Um dos meios mais eficazes de obter informações relevantes é a ingerência nas comunicações fechadas dos suspeitos (em que existe pré-determinação dos destinatários da mensagem), ou até mesmo de pessoas que se acredite estarem relacionadas com tal crime. Tal intromissão tem de ser feita, obviamente, de forma secreta, de modo a evitar o insucesso da própria investigação: se o suspeito ou pessoa investigada sabe que as suas comunicações estão a ser monitorizadas, o mais provável é que pare de as realizar, ou então que revele informações falsas de modo a inquinar o rumo da investigação propositadamente.

Hoje é inegável a importância que a Internet tem na vida e comunicação dos indivíduos, o que se reflete a nível mundial, tendo a investigação criminal muito a ganhar se considerar tais comunicações, principalmente quando os indivíduos pretendem que essas sejam fechadas. A presente investigação tem como foco o estudo sobre os meios de obtenção de prova que se relacionam com a ingerência no conteúdo das comunicações eletrónicas, possibilitadas através da Internet, em Portugal. O seu mote prende-se com o facto de no ordenamento jurídico português serem consagrados diversos meios de obtenção de prova que se relacionam com a ingerência no conteúdo das comunicações eletrónicas, muitas vezes com soluções díspares entre si.

De maneira a compreender as soluções encontradas pelo legislador português nesta matéria, é necessário estudar os diferentes meios de obtenção de prova consagrados, como as escutas telefónicas e outros meios consagrados no Código de Processo Penal, bem como os elencados na Lei do Cibercrime. Assim, a investigação criminal, doutrina e jurisprudência poderão ter mais certezas no momento de escolher qual o meio de obtenção de prova adequado, de modo a respeitar os trâmites legais exigidos pelo respeito pelos direitos fundamentais dos indivíduos, essenciais num Estado de Direito.

Palavras-chave: direito processual penal; comunicações eletrónicas; comunicações fechadas; métodos ocultos de obtenção de prova; direitos fundamentais; escutas telefónicas; Lei do Cibercrime.

Abstract

Criminal investigation often depends on the suspect's contribution to find answers to the questions raised by the commitment of a crime. One of the most effective means of obtaining relevant information is the interference in the suspect's communications (mainly when there is a pre-determined circle of recipients) or even in any other person under the investigation, necessarily related to that crime. Such intrusion has to be made in a secret way of course, in order to prevent the failure of the investigation itself: if the suspect or person under investigation knows that is being monitored in his communications, it is most likely to stop doing them or mislead the investigation on purpose.

Nowadays it's undeniable the importance of the Internet in everyone's communications worldwide, that's why the criminal investigation has a lot to gain if it considers its contents, mainly in the case of closed communications. The present work aims to study the means of obtaining evidence that relate to such communications powered by the Internet, in Portugal. Its motto is that Portuguese legal order regulates the mean of obtaining evidence by interfering in electronic communications in different ways, having different solutions in different legal acts.

In order to understand the legal solutions found by the Portuguese legislator, it is necessary to study the different means of obtaining evidence enshrined in the Portuguese law, such as the telephone tapping and others enshrined in code of criminal procedure as well as the ones listed in the Cybercrime Law. Doing so, the criminal investigation, doctrine and jurisprudence will have more certainties when it comes to the moment of choosing and respecting the legal procedures, demanded by the fundamental rights of the individuals, inherent to the rule of law.

Key-Words: criminal law, electronic communications, closed communications, secret means of obtaining evidence, fundamental rights, telephone tapping, code of criminal procedure, cybercrime law.

Índice

Introdução

Muito se discute, hoje em dia, acerca do papel da Internet na vida dos cidadãos. Que invadiu todos os seus domínios, seja a nível pessoal ou profissional, afirmando-se, entre outras coisas, como motor de busca e de comunicação preferencial.

Tratando-se a Internet de um meio de comunicação com reconhecida importância para os cidadãos, sendo milhões os utilizadores deste tipo de tecnologia, é necessário que a investigação criminal também o assuma: é inegável o potencial que a ingerência da investigação criminal no conteúdo das comunicações fechadas entre os indivíduos investigados pode ter. Afinal, se pode confidenciar-se qualquer tipo de informação relacionada com a prática de ilícitos criminais através de cartas ou telefonemas, também o pode fazer-se através destes novos meios de comunicação, possibilitados através da Internet, quer seja através do correio eletrónico ou de mensagens escritas, utilizando aplicações como o *FacebookMessenger* ou o *WhatsApp*, seja através de chamadas de voz, utilizando o *Skype*, o *WhastApp*, o *Viber*, etc.

Assim, no quadro da investigação criminal, têm de ser consideradas as comunicações que, hoje, são possíveis de realizar através da Internet, de modo a equacionar-se a sua ingerência e recolha para o processo criminal – o que poderá fazer-se, necessariamente, através de métodos ocultos de obtenção da prova, sendo vital que tal ingerência se dê sem que os interlocutores disso tenham conhecimento, só assim possuindo maior fiabilidade e relevância para a investigação.

Com a utilização de métodos ocultos de investigação para a ingerência deste tipo de comunicações, é necessário encarar as várias questões que com ela se impõem, designadamente no que respeita à violação dos direitos fundamentais dos cidadãos investigados (e que com eles estabelecem conversações), como o direito à reserva da intimidade da vida privada, o direito à palavra, o direito à inviolabilidade do domicílio e da correspondência, em especial das telecomunicações e demais meios de comunicação, o princípio *nemo tenetur se ipsum accusare* e o direito à autodeterminação informacional.

O mote para a presente investigação prende-se com a crescente importância que as comunicações eletrónicas possuem na vida dos cidadãos, mas também a existência, no nosso

ordenamento, de diferentes soluções para qual seja o meio (ou meios?) de obtenção de prova adequado para a recolha do conteúdo das conversações eletrónicas. Por um lado, o legislador, no artigo 189.º n.º 1 do Código de Processo Penal, estende à ingerência nestas comunicações o regime das escutas telefónicas – sem distinguir que tipos de comunicações eletrónicas a este regime estão submetidas: chamadas de voz através da Internet, ou também mensagens de texto trocadas instantaneamente e correio eletrónico? Por outro lado, o legislador consagra em Lei especial meios de obtenção de prova que se dirigem especificamente às comunicações eletrónicas, esquecendo-se de compatibilizar as soluções consagradas com o Código de Processo Penal.

Nesse sentido, é de fundamental importância analisar os diferentes regimes nos quais o legislador faz referência à ingerência no conteúdo das comunicações eletrónicas, para determinar qual é o regime que deve guiar a investigação criminal no seu dia-a-dia, eliminando confusões de regimes e violações do princípio da legalidade, essencial num Estado de Direito.

Assim, será necessário analisar o regime das escutas telefónicas e dos meios de obtenção de prova consagrados na Lei do Cibercrime. Para esta última análise, sempre será necessário compreender o trilho legislativo que conduziu à consagração da Lei do Cibercrime, bem como a referência a Leis avulsas conexas com a temática, tal como a Lei 32/2008, cujo objetivo foi transpor para o ordenamento português a Diretiva 2006/24/CE, considerada em 2014 inválida pelo Tribunal de Justiça da União Europeia – e que até hoje não foi objeto de qualquer alteração (ou até mesmo atenção?) por parte do legislador.

Pretende-se, assim, analisar os regimes existentes no ordenamento português que versam sobre a matéria, procurando, humildemente, traçar as linhas que devem guiar o intérprete nesta temática – linhas que por vezes se entrelaçam e complicam em muito o trabalho daqueles que tentam compreender e mesmo aplicar tais soluções.

Capítulo I - A comunicação na Sociedade da Informação e o seu impacto no Direito

> "Assumir os desafios que a história traz a si mesma e com isso a tudo aquilo que ela envolve é tarefa do nosso tempo".
>
> José de Faria Costa[1]

1. A comunicação na Sociedade da Informação

A realidade do Homem é marcada pela comunicação. Como bem refere Faria Costa, o "falar" constitui um "agir tão típico e tão profundamente anichado na estritura nuclear do ser-pessoa que, em termos onto-antropológicos, não é descabido (…) conceber-se o Homem, não só como ser-pensado, porque ser-falado, mas também enquanto estrutura aberta e porosa que, na sua hominal incompletude, só pode ser percebida pelo diálogo ou com o diálogo"[2].

Assim, desde sempre o Homem procurou desenvolver canais para comunicar com os outros, de modo a que a transmissão da informação se desse de modo preciso e completo, para se realizar enquanto "ser-pensado", que o distingue de todos os outros animais[3]. Para uma correta interpretação do que seja a "comunicação" de que depende o Homem, sempre será necessária uma clarificação concetual. A intenção de comunicar pode ter no seu reduto a transmissão da informação a um círculo pré-determinado de destinatários pelo interlocutor, tratando-se de uma comunicação (que se pretende) fechada; ou pelo contrário, pode ser marcada pela indeterminação dos destinatários da mensagem *a priori*, pretendendo-se que seja aberta[4]. Desta forma, os canais que historicamente se foram encontrando para a transmissão de informação não eram um fim em si mesmos, mas sim – e sempre – um meio

[1] Costa, José Francisco de Faria. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998. Página 141.
[2] Costa, José Francisco de Faria. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998. Página 39.
[3] Costa, José de Faria. "As telecomunicações e a privacidade: o olhar (in)discreto de um penalista." Em *As telecomunicações e o Direito na Sociedade da Informação*, de Instituto Jurídico da Comunicação, 49-78. FDUC, 1999. Página 50.
[4] São "exemplos de escola" de comunicações abertas a imprensa, o rádio e a televisão.

de concretizar a finalidade última de permitir transmissão do fluxo informacional[5]: é este que "se projeta, ajuda a construir e se densifica nos valores da palavra e da privacidade de cada um dos sujeitos interventores desse diálogo fechado"[6], e mesmo que "aberto".

A comunicação entre os sujeitos pode dar-se através da palavra falada, escrita e, a partir dos desenvolvimentos tecnológicos a que se assiste desde o final do século XX, virtual. É inegável o caráter fugaz e transitório da palavra falada, enquanto não é gravada por qualquer aparelho com essa capacidade ou reduzida a escrito após a sua emissão. Por isso a palavra escrita desde sempre se afirmou como um meio de comunicar mais ponderado, perene e duradouro porque consistente num suporte físico, não dependendo das vicissitudes da memória. Assim, "enquanto a perceção do conteúdo informacional veiculado pela palavra falada exigia a presença física do outro[7], o conteúdo informacional presente na palavra escrita – para lá da perenidade que ganhava na consistência do suporte físico – podia distanciar-se do seu autor, percorrer quilómetros, que esse afastar-se não diminuía, em um grão que fosse, a quantidade de informação cristalizada nas primeiras palavras escritas"[8]. Quanto à palavra digital, trata-se de uma inovação trazida pela "informatização em rede", que "veio trazer a possibilidade de a palavra não ser escrita, nem falada, estar virtualmente visível num écran por força de um jogo complexo cingido à simples lógica binária"[9].

A sociedade hodierna é caracterizada pela importância que dá aos meios de obter e transmitir a informação de forma instantânea e abrangente – quer quanto à informação transmitida, quer quanto aos possíveis destinatários da mesma –, sendo esta "considerada um

[5] Costa, José Francisco de Faria. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998. Página 88. No mesmo sentido entende o Autor em Costa, José de Faria. "As telecomunicações e a privacidade: o olhar (in)discreto de um penalista." Em *As telecomunicações e o Direito na Sociedade da Informação*, de Instituto Jurídico da Comunicação, 49-78. FDUC, 1999. Página 58.
[6] Costa, José Francisco de Faria. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998. Página 88.
[7] Pelo menos enquanto não foi inventado o telefone, e outros aparelhos com a capacidade de transmitir mensagens de voz – em tempo real ou gravado.
[8] Costa, José de Faria. "As telecomunicações e a privacidade: o olhar (in)discreto de um penalista." Em *As telecomunicações e o Direito na Sociedade da Informação*, de Instituto Jurídico da Comunicação, 49-78. FDUC, 1999. Página 54.
[9] Costa, José de Faria. "As telecomunicações e a privacidade: o olhar (in)discreto de um penalista." Em *As telecomunicações e o Direito na Sociedade da Informação*, de Instituto Jurídico da Comunicação, 49-78. FDUC, 1999. Página 56.

recurso estratégico primordial e indispensável para o seu próprio desenvolvimento"[10]. Vivemos hoje a Sociedade de Informação – que se afirmou, essencialmente, a partir da década de 70 do século passado[11], e que constitui um "novo paradigma de sociedade, no qual a energia é progressivamente substituída pela informação, como fonte primeira do progresso social"[12]. Assim, a "Sociedade de Informação – expressão que cada vez importa menos definir na medida em que se vai vivendo em maior escala – assenta sobre o uso ótimo das novas tecnologias da informação e da comunicação, em respeito pelos princípios democráticos, da igualdade e da solidariedade, visando o reforço da economia e da prestação de serviços públicos e, a final, a melhoria da qualidade de vida de todos os cidadãos"[13].

Com o desenvolvimento tecnológico e comunicacional a que se assiste, todos os domínios se têm melhorado e desenvolvido, do qual as telecomunicações não são exceção. As comunicações realizam-se, hoje, através da fibra ótica, tendo a utilização do cobre sido substituída, bem como por satélite e através da Internet. Tendo a sua origem no contexto da Guerra Fria, a 1 de janeiro de 1983 nasceu oficialmente a Internet[14], e trata-se de uma "interconexão de redes, tornada possível através de um protocolo denominado TCP/IP (o Transport Control Protocol/ Internet Protocol), uma espécie de língua comum que permite a comunicação entre as redes, quaisquer que sejam as suas caraterísticas tecnológicas"[15]. É por isso uma "rede de computadores à escala mundial, que entre si comunicam utilizando uma especial linguagem informática"[16].

---

[10] Como se retira e infere de Casimiro, Sofia de Vasconcelos. *Mapa da problemática jurídica da Sociedade da Informação.* Vol. IX, em *Direito da Sociedade de Informação*, de AA VV, 31-55. Coimbra Editora, grupo Wolters Kluwer, 2011. Página 32.

[11] Como refere Benjamin da Silva Rodrigues, em Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 37.

[12] Marques, Garcia, e Lourenço Martins. *Direito da Informática.* Coimbra: Almedina, 2000. Página 42.

[13] Marques, Garcia, e Lourenço Martins. *Direito da Informática.* Coimbra: Almedina, 2000. Página 43.

[14] Que ocorreu quando se deu a transição entre o sistema da ARPANET ("que ligava departamentos de pesquisa governamentais e investigadores com projetos na área militar em várias universidades à própria ARPA") ao sistema TCP/IP – como se retira de Castro, Catarina Sarmento e. "Protecção de dados pessoais na Internet." *Revista Sub Judice*, Setembro de n.º 35, 2006: 11-29. Página 13.

[15] Marques, Garcia, e Lourenço Martins. *Direito da Informática.* Coimbra: Almedina, 2000. Página 43.

[16] Castro, Catarina Sarmento e. "Protecção de dados pessoais na Internet." *Revista Sub Judice*, Setembro de n.º 35, 2006: 11-29. Página 13.

Com a Internet, nascem inúmeros modos de comunicar, nascendo novos meios de comunicação[17] até então impensáveis: tornou-se possível a transmissão quase (?) instantânea de informação, esbatendo-se as fronteiras físicas que outrora separavam as pessoas – em segundos, qualquer informação, som, imagem ou mensagem pode chegar a qualquer parte do mundo, desde que possua conexão à *rede das redes*. Assim, "a internet tornou-se um canal cada vez mais importante para a totalidade dos serviços de telecomunicações existentes, incluindo os serviços telefónicos convencionais, de tal modo que os operadores de telecomunicações tiveram, de um dia para o outro, de «saltar(em) para o comboio em andamento da Internet»"[18]. Isto porque até as chamadas de voz (e também imagem) se podem realizar através da Internet, através do sistema *Voice Over IP*. Atualmente, a "banda larga assegura Internet cada vez mais rápida e os avanços tecnológicos tornaram-na omnipresente: a Internet já fugiu ao computador, está na TV interativa, e em movimento nos aparelhos móveis de telecomunicações de terceira geração"[19].

É inegável que o digital e informático fazem parte da vida de todos nós, tendo alterado até o mais pequeno dos hábitos humanos[20]: trabalhamos e comunicamos através da Internet, e até nas atividades de lazer ela é imprescindível. Já não se perguntam conselhos a amigos de sítios para onde ir, nem direções em estradas desconhecidas – recorre-se a aplicações informáticas que possuem todas as informações e comentários relativos a qualquer local ou estabelecimento, sendo a "indicação" dos caminhos feita de modo interativo, através do recurso ao *Global Positioning System*. Já não se trocam cartas com parentes distantes, nem se reduzem os contactos devido aos elevados custos das chamadas internacionais – vários

[17] Como se retira de: Costa, José Francisco de Faria. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998. Página 86 e seguintes, é necessária a diferenciação concetual e dogmática dos conceitos de comunicação e meios de comunicação, entre os quais intercede uma "diferença radical": "a comunicação é um conceito relacional, enquanto os meios de comunicação devem ser olhados ou valorados como conceitos instrumentais. Se se pode, por consequência, avançar com a ideia de que *communicatio est relatio*, tal resulta tanto da afirmação indesmentível da dimensão onto-antropológica que podemos surpreender no nosso modo-de-ser comunitário, como também da incontornável manifestação fonética que dos atos comunicacionais se pode captar, apreender ou experienciar". Por outro lado, os meios de comunicação possuem uma inalienável vertente instrumental, de modo a constituir-se como "elos de ligação pelos quais corre o fluxo informacional que permite o ato comunicacional".

[18] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 44.

[19] Castro, Catarina Sarmento e. "Protecção de dados pessoais na Internet." *Revista Sub Judice*, Setembro de n.º 35, 2006: 11-29. Página 13.

[20] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I*, A *monotorização dos fluxos informacionais e comunicacionais*. Coimbra: Coimbra Editora, 2008. Página 26.

aplicativos informáticos permitem a troca de e-mails ou mensagens instantâneas para as partes mais remotas do globo, e também a realização de chamadas de voz e vídeo.

Como facilmente se constata, com a Internet e o advento das tecnologias da informação e da comunicação (TIC), foram paulatinamente abolidas as fronteiras físicas que outrora separavam os indivíduos, passando estes a estar "à distância de um clique", reunidos num lugar transcendente e global, sem paralelo – o ciberespaço. Assiste-se à "democratização da informação e das comunicações, verificando-se a abolição de fronteiras até aí inultrapassáveis"[21]. Nasceram formas de comunicar *ex novo*, sem qualquer comparação com os meios existentes até então, permitindo-se a comunicação à distância de forma instantânea (sendo meras frações de segundos que separam o envio de uma mensagem e a sua receção no terminal de destino) e com baixos custos associados, até qualquer parte do mundo, devido à expansão e afirmação global da Internet[22].

Foi assim alterado o paradigma comunicacional e informacional que se vivia até então, afirmando-se as comunicações eletrónicas, realizadas através da Internet: chamadas de voz e imagem através do sistema de *Voice over IP* (de que são exemplo o *Skype* e o *FaceTime*), o correio eletrónico[23] e mensagens instantâneas trocadas através de aplicações como *Facebook Messenger* ou o *WhatsApp*.

Do ponto de vista jurídico, são vários os problemas que a Internet e a revolução nas telecomunicações vieram introduzir na Sociedade de Informação: "as tecnologias da informação e da comunicação podem ser utilizadas enquanto instrumentos (muitas vezes mais eficazes quer nos danos causados quer no encobrimento da identidade dos seus autores)

---

[21] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 27.

[22] Nesse sentido entente Oliveira Ascensão: "A chamada sociedade de informação trouxe uma pletora insuspeitada de novos meios de comunicação. Por via deles, as possibilidades de expressão multiplicaram-se. Não é assim despropositado afirmar-se que os novos meios servem a liberdade de expressão", em Ascensão, José de Oliveira. *A sociedade da informação.* Vol. I, em *Direito da Sociedade da Informação*, de AA VV, 163-184. Coimbra: Coimbra Editora, 1999. Página 165.

[23] Que para Adelaide Menezes Leitão, se tratou de um marco na revolução das comunicações, que só encontra paralelo na "invenção do telefone por Bell", uma vez que "permite não só partilhar o som, mas ainda aceder a imagens e a textos. Além disto, enquanto uma chamada telefónica, depois de realizada, desaparece instantaneamente, nos e-mails pode ficar uma cópia no administrador, devido aos *back ups* que são automaticamente efetuados pelo sistema - Leitão, Adelaide Menezes. *Metatags e o correio eletrónico entre os novos problemas do direito da internet.* Vol. IV, em *Direito da Sociedade da Informação*, de AA VV, 405-432. Coimbra: Coimbra Editora, 2003. Página 426.

para a prática de crimes usuais da realidade corpórea e cujo tipo legal está previsto sem considerar a utilização dos meios tecnológicos como um elemento integrador do crime"[24]. Surgem problemas como o perigo trazido pela informatização em rede dos dados pessoais dos indivíduos, que pode acarretar graves violações aos seus direitos fundamentais, nomeadamente a sua privacidade[25] "informacional e comunicacional"[26], problemas derivados da "formação de contratos *on-line*, com a publicidade não solicitada (*spam* e *junk mail*) e com outras situações que, a todo o momento, se vão colocando como resultado direto da circulação de informação gerada pela sua facilidade e rapidez"[27]. Para além disso, os Estados são confrontados com problemas como o terrorismo, que encontram na Internet um veículo bastante eficaz e potenciador de ameaças globais, deparando-se "com a problemática de estabelecerem um equilíbrio entre a liberdade individual dos seus cidadãos e a segurança dos Estados"[28].

Porque pensamos, tal como Faria Costa, que "é dever de todo o investigador – por mais simples e elementar que seja aquilo que quer apresentar (…) tornar claro qual ou quais as finalidades últimas do seu estudo"[29], no que à presente investigação diz respeito importa dirigir a atenção a uma questão específica: a interceção do conteúdo de comunicações escritas ou faladas, realizadas através da Internet e que se pretendem fechadas entre os indivíduos, no âmbito da investigação criminal. E esta questão terá de ser analisada sob dois prismas: quer do lado do investigado, que através da monitorização das suas comunicações vê comprimidos alguns dos seus direitos, erigidos pela Constituição como fundamentais (como o por exemplo o direito à palavra, a reserva da intimidade da vida privada e a inviolabilidade das suas comunicações); quer do lado do Direito Processual Penal, a sua *ratio* e limites: devido aos

[24] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 18.
[25] Para mais desenvolvimentos sobre o tema, consultar, entre outros, Leitão, Adelaide Menezes. *Metatags e o correio eletrónico entre os novos problemas do direito da internet.* Vol. IV, em *Direito da Sociedade da Informação*, de AA VV, 405-432. Coimbra: Coimbra Editora, 2003.
[26] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 45.
[27] Leitão, Adelaide Menezes. *Metatags e o correio eletrónico entre os novos problemas do direito da internet.* Vol. IV, em *Direito da Sociedade da Informação*, de AA VV, 405-432. Coimbra: Coimbra Editora, 2003. Página 426.
[28] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 45.
[29] Costa, José Francisco de Faria. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998. Página 121.

progressos técnicos a que se tem assistido, com o aparecimento de novos meios de intercetar as comunicações no âmbito da investigação criminal (e até mesmo fora dela[30]), é necessária a sua consagração legal – pois se nascem novos meios de comunicar à escala planetária, nascem, na mesma medida, múltiplos modos de intercetar essas comunicações. E para que tal monitorização de comunicações seja válida e as provas passíveis de ser valoradas por qualquer Tribunal, estritos parâmetros legais pré-estabelecidos terão de ser respeitados.

2. A comunicação e a Constituição da República Portuguesa

Antes de qualquer análise ao regime português que verse sobre as ingerências nas comunicações dos indivíduos – sem esquecer que nos dedicamos às comunicações eletrónicas, potenciadas pelo recurso à Internet – no contexto de uma investigação criminal, potencialmente lesiva de direitos fundamentais reconhecidos e valorizados pela sociedade, sempre será necessário realizar um estudo sobre esses mesmos direitos, averiguando a sua esfera de proteção, para se poder estar em condições de averiguar pela possível, necessária e adequada compressão daqueles no contexto de uma investigação criminal.

Esta análise é bastante importante devido ao modo como as ingerências nas comunicações são feitas: de modo secreto e sem que os "escutados" disso tenham conhecimento, estando livres para dizer o que querem sem ter consciência da implicação do que estão a dizer – podendo levar, inclusivamente, à sua autoincriminação, tornando "os convencionais direitos dos arguidos obsoletos"[31]. Para além disso, a vigilância de comunicações é abrangente, incidindo sobre um indeterminável número de escutados *a priori*, bem como potenciador de revelação de inúmeras informações relativas "não apenas ao passado, mas em especial ao futuro ou ao tempo prévio e posterior aos factos", incluindo

[30] Não sendo de estranhar que "a consciência coletiva se sinta cada vez mais ameaçada. Não por um Estado leviatânico, mas por uma sociedade que dá a possibilidade, a cada um dos seus membros, de espiolhar ao milímetro o guião da vida de quem quer que seja e até de descobrir as frustrações ou os anseios mais íntimos da vida dos seus concidadãos" – conforme constata Faria Costa, em Costa, José de Faria. "As telecomunicações e a privacidade: o olhar (in)discreto de um penalista." Em *As telecomunicações e o Direito na Sociedade da Informação*, de Instituto Jurídico da Comunicação, 49-78. FDUC, 1999. Página 66.

[31] Albrecht, Hans-Jörg. "Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos." Em *Que futuro para o direito processual penal?* , de Mário J. Ferreira Monte, 725-743. Coimbra Editora, 2009. Página 726.

"informações independentemente do direito de não prestar declarações das testemunhas"[32], e "independentemente da intimidade e fiabilidade da comunicação"[33] – ou seja, aqueles que se poderiam recusar a testemunhar em sede de audiência de julgamento, podem ser escutados durante a fase de investigação e contribuir para a incriminação do suspeito, mesmo que as informações transmitidas não sejam verdadeiras ou de pouca fiabilidade.

Tratando-se de uma inevitável colisão de dois interesses – por um lado, a procura da verdade que rege a investigação criminal, e, por outro, os direitos fundamentais dos indivíduos, sempre se terá de traçar um critério de ponderação que permita conciliar estes dois interesses, ambos pilares essenciais de um Estado de Direito Democrático, estabelecendo os casos em que seja ou não razoável a compressão dos direitos fundamentais dos indivíduos em prol dos fins da investigação criminal.

Em algumas décadas assistiu-se à "emergência e triunfo de direitos como a palavra, a imagem, a autodeterminação informacional, a identidade genética e, a iniciar agora o seu caminho, a integridade confidencialidade dos sistemas informáticos"[34], e se "de um lado, a progressão – expressa na emergência e triunfo de novos direitos fundamentais ou de novas dimensões dos direitos preexistentes – é espontânea, contínua e automática, apenas dependendo da atualização da consciência jurídica, às mãos da doutrina e da jurisprudência (constitucionais)", "do outro lado, o caminho – *sc.* a consagração de novos meios de obtenção de provas resultantes do aproveitamento das possibilidades de intervenção e intromissão oferecidas pelas realizações técnico-científicas – faz-se de forma descontínua e derivada, ao ritmo das sucessivas e localizadas intervenções do legislador"[35].

[32] Albrecht, Hans-Jörg. "Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos." Em *Que futuro para o direito processual penal?* , de Mário J. Ferreira Monte, 725-743. Coimbra Editora, 2009. Página 726.
[33] Albrecht, Hans-Jörg. "Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos." Em *Que futuro para o direito processual penal?* , de Mário J. Ferreira Monte, 725-743. Coimbra Editora, 2009. Página 726.
[34] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 149.
[35] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 148.

a) O direito geral de personalidade – o artigo 26.º Constituição da República Portuguesa

Consideramos, acompanhando os ensinamentos de Jorge Miranda e Rui Medeiros, que o "artigo 26.º constitui expressão direta do postulado básico da dignidade humana que a Constituição consagra logo no artigo 1.º como valor logicamente anterior à própria ideia de Estado de Direito democrático e que constitui a referência primeira em matéria de direitos fundamentais"[36]. O direito geral de personalidade abrange a tutela de "todos os bens de personalidade independentemente de estarem ou não tipicamente consagrados"[37], e, entre outras dimensões, o direito geral de personalidade refere-se explicitamente ao direito à palavra e à imagem, que se considera como "expressões típicas da autonomia pessoal", direitos que incluem "o direito a que não sejam registadas ou divulgadas palavras ou imagens da pessoa sem o seu consentimento, conferindo assim um direito à «reserva» e à «transitoriedade» da palavra falada e da imagem pessoal"[38].

i. Direito à reserva da intimidade da vida privada

O direito à reserva da intimidade da vida privada e familiar[39] é uma das dimensões do direito geral de personalidade abrangidas pelo artigo 26.º CRP, que é referida também em normativos internacionais, como o artigo 12.º da Declaração Universal dos Direitos do Homem, o artigo 8.º da Convenção Europeia dos Direitos do Homem, no artigo 7.º da Carta de Direitos Fundamentais da União Europeia e no artigo 17.º do Pacto Internacional relativo aos direitos civis e políticos.

---

[36] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 603.

[37] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 607.

[38] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 618.

[39] É usual os Autores recorrerem à "Teoria das Três Esferas" para a concretização do que seja a dimensão de reserva da intimidade da vida privada e familiar, que, apesar de não ser o objeto do presente estudo, sempre merecerá uma breve referência: "esfera íntima corresponde ao núcleo duro do direito à intimidade da vida privada; a esfera privada admite ponderações de proporcionalidade; na esfera social estaremos já no quadro do direito à imagem e à palavra e não do direito à intimidade da vida privada" - Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 620.

Este direito "compreende, em qualquer caso, não somente o direito de oposição à divulgação da vida privada (*public disclosure of private facts*), mas também o direito ao respeito da vida privada, ou seja, o direito de oposição à investigação sobre a vida privada (*intrusion*)"[40]. Por outro lado, este direito também confere aos indivíduos o poder de controlar as informações que a eles disserem respeito, inserindo-se também no âmbito de um direito mais amplo, de autodeterminação informacional (que será analisado infra).

Para Conde Correia, a "vida privada compreende aqueles factos, atitudes ou opiniões individuais e particulares, que não tenham qualquer relação com a vida pública e que possam, em determinado momento histórico, ser razoavelmente considerados confidenciais, por forma a impedir ou restringir a sua divulgação"[41]. Conforme este Autor, "um dos interesses que estão subjacentes à proteção da reserva da intimidade da vida privada e familiar é obstar, ou pelo menos, supervisionar o acesso ou o conhecimento de informação pertinente à vida privada ou familiar de outrem e de impedir ou controlar a divulgação da mesma, ainda que licitamente obtida". Para além disso, há também o interesse de "furtar-se à atenção dos outros (anonimato) e o de não permitir o acesso dos outros a si próprio (*solitude*)"[42].

Assim, está bom de ver que o direito à reserva da intimidade da vida privada é um direito fortemente afetado quando são autorizadas investigações, no âmbito de um processo de natureza criminal, que permitam a ingerência na vida privada dos sujeitos, ainda que perante o caso concreto tenha de "ceder" em razão das finalidades da investigação criminal, sendo a medida validamente ponderada, proporcional e autorizada, sendo por isso realizada de forma lícita – uma vez que a sua intimidade fica exposta, com a agravante do desconhecimento dessa mesma ingerência.

[40] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 620.
[41] Correia, João Conde. "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?" *Revista do Ministério Público nº 79*, Julho/Setembro de Ano 20, 1999: 45-67. Página 49.
[42] Correia, João Conde. "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?" *Revista do Ministério Público nº 79*, Julho/Setembro de Ano 20, 1999: 45-67. Página 48.

ii. Direito à palavra

Conforme assinalado no ponto anterior, o direito à palavra é uma das dimensões do direito geral de personalidade consagrado no artigo 26.º CRP. No entanto, e seguindo o entendimento de Conde Correia, consideramos que o direito à palavra não é abrangido pelo direito à reserva da intimidade da vida privada e sim um direito fundamental autónomo, pois, apesar de derivar deste, o direito à palavra, pela sua importância, ganha independência e constitui um bem jurídico com dignidade constitucional[43].

Gomes Canotilho e Vital Moreira distinguem três dimensões do direito à palavra: "direito à voz, como atributo de personalidade, sendo ilícito, sem consentimento da pessoa, registar e divulgar a sua voz (com ressalva, é claro, do lugar em que ela foi utilizada)"; "direito às «palavras ditas», que pretende garantir a autenticidade e o rigor da reprodução dos termos, expressões, metáforas escritas e ditas por uma pessoa"; e o "direito ao auditório, ou seja, a decidir o círculo de pessoas a quem é transmitida a palavra"[44]. Ou seja, podemos assim concluir que a proteção à palavra conferida pela Constituição trata-se apenas da palavra falada, e não escrita.

Concordamos com Rita Castanheira Neves quando escreve que a proteção constitucional à palavra falada se deve à sua "volatilidade e à expectativa de que a mesma não possa ser reproduzida em mais nenhum contexto espácio-temporal para além daquele em que foi proferida", protegendo-se "simultaneamente a privacidade e a palavra falada, como bens jurídicos autónomos" [45]. A palavra escrita não beneficia desta proteção, por ser mais refletida e lhe ser inerente o receio do que se vai cunhar de perenidade, devido ao suporte escrito, seja em que modalidade for, não havendo a volatilidade decorrente da comunicação oral, sendo, apesar disso, de proteger "a mesma inviolabilidade das comunicações, mas agora acompanhada da privacidade"[46]. Assim, esta Autora entende que "no âmbito da pura análise

[43] Correia, João Conde. "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?" *Revista do Ministério Público nº 79*, Julho/Setembro de Ano 20, 1999: 45-67. Página 50.
[44] Canotilho, Jorge J. Gomes, e Vital Moreira. *Constituição da República Portuguesa anotada, Vol. I.* 4ª edição revista e atualizada. Coimbra Editora, 2007. Página 467.
[45] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 46.
[46] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 47.

jurídico-penal é bastante a dualização palavra falada/palavra escrita, cabendo a palavra virtual, conforme os casos, numa ou noutra categoria"[47]. Concordamos com este entendimento, não sendo necessário autonomizar, no plano normativo, a palavra virtual, situada ao lado da palavra falada e escrita. Pois, no seu reduto, corresponde ou a uma, ou a outra. O que consideramos ser um elemento de distinção é, apenas, o meio através do qual a comunicação é veiculada: devendo, e só nesse ponto, haver distinção. Porque a nível da consagração dos direitos fundamentais na Constituição, toda a expressão humana é protegida pelo artigo 26.º CRP, sendo necessária a diferenciação na amplitude de proteção conforme seja escrita ou falada, por se considerar que esta última possui um caráter menos refletido, e sua "interceção" uma violação mais gravosa.

No entanto, será ***toda*** a palava virtual escrita que possui as características de ponderação e cuidado que lhe conferem um caráter mais refletido e justifiquem o tratamento diferenciado da palavra falada, sendo considerada a sua interceção menos lesiva dos direitos fundamentais dos indivíduos? Vejamos. Num e-mail há a necessária ponderação do indivíduo naquilo que irá escrever, pois sabe que o produto final do e-mail pode ser facilmente armazenado ou impresso, passando a constituir um documento como todos os outros. No entanto, é necessário encarar a questão de que existem atualmente programas que permitem a troca instantânea de mensagens como o *Messenger* ou o *WhatsApp –esta* palavra escrita deve beneficiar da mesma ponderação que a corrente palavra escrita, ou da especial vulnerabilidade que assiste à palavra falada? Apesar do caráter instantâneo da emissão e receção das mensagens – existindo, nos programas referidos e a título de exemplo, a possibilidade de ver que a outra pessoa está a escrever e saber instantaneamente se a mensagem foi entregue e até lida pelo destinatário, o declarante tem sempre a consciência de que está a veicular a palavra de forma escrita, que necessariamente é registada e arquivada, seja no aparelho do declarante, do declaratário ou do prestador de serviços. E esta circunstancia sempre lhe coarta alguma da volatilidade que assiste à palavra falada (que só se for gravada ou ouvida por terceiros é que é perene).

[47] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 50.

Quando realizadas comunicações através de chamadas voz possibilitadas pelo sistema *Voice over IP*, todas as dimensões do direito à palavra falada são chamadas à colação, tal como o seriam numa chamada telefónica dita tradicional, seja através do telefone fixo ou do telemóvel. A essência da comunicação é a mesma relativamente à palavra falada dita "tradicional", sendo diferentes apenas os meios técnicos através dos quais a chamada de voz se processa.

b) Direito à inviolabilidade do domicílio e da correspondência, em especial das telecomunicações e demais meios de comunicação – o artigo 34.º n.º 4 Constituição da República Portuguesa

A ingerência das autoridades públicas na correspondência dos indivíduos, nas telecomunicações ou em quaisquer outros meios de comunicação apenas é tolerada pela Constituição se consagrada na lei em matéria de investigação criminal, e respeitando escrupulosamente todos os requisitos estabelecidos pelo legislador: "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal" – artigo 34.º n .º 4 da CRP. Ultrapassado o âmbito de autorização plasmado em lei penal, está-se perante a prática de ilícitos criminais, seja quem for o agente que o pratique.

Assim, para que se consagre qualquer meio de obtenção de prova que interfira diretamente com este direito consagrado no artigo 34.º n.º 4 CRP, é necessário que se respeite o princípio da reserva de lei, plasmado no artigo 18.º n.º 2 CRP, uma vez que se trata de uma "restrição de direitos, liberdades e garantias"[48], sendo matéria de competência relativa da Assembleia da República, ainda com possibilidade de autorização ao Governo para legislar sobre a matéria – artigo 165.º n.º 1 b) CRP. No entanto, esta reserva de lei é "*suis generis*" – uma vez que a restrição não deve exceder o âmbito da investigação penal[49]. Para além da reserva legal, é também necessário que a compressão dos direitos fundamentais dos

[48] Aguilar, Francisco. "Notas reflexivas sobre o regime das escutas telefónicas no Código de processo penal português." *O Direito,* 2016 II, ano 148º: 559-583. Página 561.
[49] Nesse sentido, Aguilar, Francisco. "Notas reflexivas sobre o regime das escutas telefónicas no Código de processo penal português." *O Direito,* 2016 II, ano 148º: 559-583. Página 561.

indivíduos no que toca à sua privacidade, domicílio e comunicações, seja autorizada por um juiz – artigo 32.º n.º 4 CRP, que no caso das escutas telefónicas se encontra vertida nos artigos 187.º n.º 1 e 269.º n.º 1 e) CPP e no caso da apreensão de correspondência no artigo 179.º CPP[50].

Em suma, consideramos importante assinalar que qualquer meio de obtenção de prova que venha a constituir a exceção prevista no número 4 do artigo 34.º CRP – ou seja, que se dedique à ingerência ou monitorizações das comunicações no âmbito de telecomunicações, no caso – deve respeitar o princípio da proporcionalidade, previsto no artigo 18.º n.º 2 CRP, cujos corolários são a adequação, necessidade e proporcionalidade em sentido estrito.

Na primeira vertente do princípio da proporcionalidade, a adequação, concordamos com o brilhante entendimento de Francisco Aguilar[51], quando considera que este princípio impõe que a "restrição aos direitos, liberdades e garantias se destine à salvaguarda de outros direitos ou interesses constitucionalmente protegidos"[52] – o que, no caso do direito e processo penal consubstancia a tutela dos bens jurídicos postos em causa pela atuação que é objeto no processo – "*rectius*, na realização da justiça penal no caso concreto"[53]. Desta forma, os meios de obtenção de prova consagrados ou a consagrar no âmbito da ingerência nas comunicações têm de possuir a finalidade única de descoberta da verdade no caso concreto, no âmbito da investigação e processo em curso, devido à violação de bens jurídicos que o legislador entendeu serem merecedores de tutela penal. Entende ainda o digníssimo Professor que neste âmbito rege ainda o princípio da idoneidade do recurso ao meio de obtenção de prova para recolha desses meios de prova, sendo o meio de obtenção que se considere o meio correto e necessário para tal obtenção. Entende ser ainda fulcral o princípio da especialidade: sendo necessário um processo em curso para que o meio de interceção ou monitorização das comunicações seja autorizado e posteriormente valorado. Quanto à vertente de "necessidade" do princípio da proporcionalidade, pode ser entendido como o único e adequado meio de

[50] Infra melhor se analisará o âmbito da apreensão de correspondência e o seu alcance.
[51] Que foca o seu estudo no regime das escutas telefónicas – mas que consideramos compatível (e até necessário) para qualquer meio de obtenção de prova que se dedique à mesma realidade: interceção de comunicações.
[52] Aguilar, Francisco. "Notas reflexivas sobre o regime das escutas telefónicas no Código de processo penal português." *O Direito*, 2016 II, ano 148º: 559-583. Página 564.
[53] Aguilar, Francisco. "Notas reflexivas sobre o regime das escutas telefónicas no Código de processo penal português." *O Direito*, 2016 II, ano 148º: 559-583. Página 564.

obtenção de prova para alcançar aqueles resultados, que não se poderiam obter por outros meios, no mesmo processo. Quanto à proporcionalidade em sentido estrito, entendemos que se traduz na proporção entre o meio de obtenção de prova utilizado e os direitos restringidos pela sua utilização, o que, no caso das escutas telefónicas, se traduzem na "catalogação dos crimes escutáveis", e ao "universo dos escutados"[54].

Como constata Costa Andrade, é de grande importância a delimitação concetual do que seja a "telecomunicação" – que goza de referência em sede constitucional, no artigo 34.º CRP, e a nível penal, no artigo 194.º e 276.º CP[55], tanto para rigor terminológico, como por "continuar a deter a consistência e a autonomia categorial bastantes para sobre ele se erigir um regime processual penal geral, cobrindo também, naturalmente como domínio específico, as intromissões nas comunicações eletrónicas"[56]. Entende o Ilustre Autor que o conceito de telecomunicação abrange "todos os processos técnicos de recolha, processamento, tratamento, conservação e transmissão de dados, principalmente através de dados correspondentes a palavras ou imagens nelas convertíveis"[57]. Com a proteção das telecomunicações e a proibição expressa da ingerência nas mesmas, fora dos quadros permitidos pela legislação penal, este Mestre entende que "à semelhança do que acontece com o sigilo da correspondência, também aqui o que está em causa é assegurar o livre desenvolvimento da personalidade de cada um através da troca, à distância, de informações, notícias, pensamentos e opiniões, à margem da devassa da publicidade. O que está em causa é, em última instância, é a tutela da privacidade"[58], e, mais concretamente, a privacidade à distância.

---

[54] Aguilar, Francisco. "Notas reflexivas sobre o regime das escutas telefónicas no Código de processo penal português." *O Direito*, 2016 II, ano 148º: 559-583. Página 566.

[55] Como será analisado infra, a tipificação destes ilícitos criminais visa a proteção da inviolabilidade da correspondência, que se relaciona com "o direito que assiste aos cidadãos de manifestarem livremente as suas opiniões e convicções de forma também ela reservada" – tal como entende Paula Ribeiro de Faria em Dias, Figueiredo. *Comentário Conimbricense ao Código Penal, Parte Especial.* Vol. Tomo II. Coimbra Editora, 1999. Página 905.

[56] Retirado de Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 157.

[57] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 146.

[58] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 158.

Uma vez que é necessária a introdução de um terceiro que permita a realização técnica da conversação, nomeadamente uma empresa de telecomunicação, existe uma "específica situação de perigo decorrente do domínio que o terceiro detém – e enquanto detém – sobre a comunicação"[59] – pois este domínio assegura-lhe a "possibilidade fática de intromissão arbitrária". Afirma-se por isso o sigilo das telecomunicações – que "visa proteger a confiança na segurança e reserva nos sistemas (empresas) de telecomunicações"[60]. Este sigilo não é violado se um dos interlocutores da conversação, sem que o outro saiba, divulgue o conteúdo da informação ou permita a ingerência de um terceiro na mesma. É importante realçar que o sigilo das telecomunicações "só existe enquanto dura o processo dinâmico de transmissão, isto é, até ao momento em que a comunicação entra na esfera de domínio do destinatário"[61] – se a mensagem é recebida e lida pelo destinatário, deixa de existir o processo de transmissão da mensagem, e bem assim termina a "específica situação de perigo" em que o interlocutor se encontra.

Conde Correia prefere falar do "direito ao sigilo da correspondência e de outros meios de comunicação privada", que acompanhamos, uma vez que, com essa terminologia, o direito "protege toda a espécie de comunicação interpessoal, privada ou não, efetuada por intermédio da correspondência e das telecomunicações, independentemente do meio técnico utilizado ou do seu conteúdo"[62], reportando-se à comunicação fechada. Este direito visa tutelar a confiança na privacidade que se exprime através da correspondência ou das telecomunicações, de modo a que não exista conhecimento "ou divulgação a terceiros que deve emergir de qualquer sistema organizado de correspondência e telecomunicações num Estado Democrático e que é condição do livre desenvolvimento da personalidade humana"[63]. Este direito, ao mesmo tempo que impede precisamente qualquer ingerência, violação e

[59] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 158.
[60] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 158.
[61] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 159.
[62] Correia, João Conde. "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?" *Revista do Ministério Público nº 79*, Julho/Setembro de Ano 20, 1999: 45-67. Página 51.
[63] Correia, João Conde. "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?" *Revista do Ministério Público nº 79*, Julho/Setembro de Ano 20, 1999: 45-67. Página 52.

devassa por qualquer indivíduo – terceiro ou o Estado – impõe sobre todos os que à correspondência ou telecomunicação tenham acesso a proibição da sua divulgação.

Outro aspeto a assinalar é que o direito ao sigilo das telecomunicações abrange não só os dados de conteúdo da comunicação, mas também os dados ou circunstâncias da comunicação, nomeadamente os dados de base e os dados de tráfego. Os dados de conteúdo são os respeitantes ao "próprio conteúdo da comunicação, à mensagem em si mesma considerada"[64] – dados a que nos reportamos no presente trabalho. Os dados de base são "os dados instrumentais da comunicação, tais como o posto e o numero de acesso, a identificação do utilizador ou da sua morada", os "dados que permitem a ligação à rede"[65]. Por sua vez, os dados de tráfego "os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente"[66].

Podemos assim afirmar que a abertura constitucional do artigo 34.º n.º 4 CRP permitiu a criação de específicos tipos de ingerência nas comunicações: "i) a ingerência nas comunicações postais e telegráficas, *rectius*, correspondência – comunicação escrita; ii) a ingerência nas comunicações telefónicas – comunicações orais"; "a ingerência nas comunicações não telefónicas mas a elas equiparadas – correio eletrónico, comunicações telemáticas e outras; iv) a ingerência nas comunicações entre presentes – captação em ambiente físico, fora das redes de comunicações eletrónicas"[67]. Será esta abertura constitucional o objeto do presente estudo – no que contende com a ingerência pela investigação criminal nas comunicações eletrónicas (e fechadas) dos indivíduos.

[64] Santos, Cristina Máximo dos. "As novas tecnologias da informação e o sigilo das telecomunicações." *Revista do Ministério Público nº 99*, Julho/Setembro de Ano 25, 2004: 89-116. Página 95.
[65] Santos, Cristina Máximo dos. "As novas tecnologias da informação e o sigilo das telecomunicações." *Revista do Ministério Público nº 99*, Julho/Setembro de Ano 25, 2004: 89-116. Página 95.
[66] Conforme o disposto no artigo 2.º c) da Lei 109/2009. O artigo 2.º c) da Lei 41/2004 apresenta uma definição para dados de tráfego mais incompleta: "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma".
[67] Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 127.

c) A "Constituição processual penal" – em especial, o artigo 32.º n.º 8 Constituição da República Portuguesa

Realçando a proteção que confere ao sigilo das comunicações, a Constituição vem ainda consagrar como nulas todas as provas obtidas mediante a intromissão abusiva nas mesmas, no importantíssimo artigo 32.º n.º 8 CRP: ou seja, todas as provas obtidas por meios que não estejam previstos na lei – e ainda que o estejam, mas que não sejam necessárias, adequadas e proporcionais (artigo 18.º n.º 2 e 3 CRP, princípio da proporcionalidade). Existe assim uma clara proibição de prova[68], ancorada na ilegítima intromissão das comunicações dos indivíduos, seja por que meio esta se realizar, ficando assim "demonstrada, mais uma vez, a constante tensão dialética entre a proteção da reserva da intimidade da vida privada e os meios postos ao dispor da justiça penal para alcançar a descoberta da verdade material"[69] – que, não se esqueça, tem também de ser processualmente válida.

Importa ter em mente que "o direito processual penal é direito constitucional aplicado" – uma vez que o "direito processual penal anda estreitamente associado à Constituição, desde a origem do constitucionalismo, ao ponto de já ter sido considerado o verdadeiro «sismógrafo» de uma lei fundamental: «a cada nova ordem constitucional, um novo direito processual penal»"[70]. Assim, é grande a preocupação constitucional sobre as normas criminais, "e que à medida que se vão aprofundando ou desenvolvendo os direitos, liberdades e garantias das pessoas também se vão aprofundando e desenvolvendo as normas da *constituição processual penal*"[71].

O artigo 32.º CRP é a pedra de toque de todo o processo penal, a referida *constituição processual penal* – uma vez que consagra os princípios que devem reger a sua tramitação e realização, e o seu número 8 plasma a ideia de que são inaceitáveis determinadas provas e

[68] A que também se faz referência nos artigos 5.º e 12.º da Declaração Universal dos Direitos do Homem, artigos 3.º e 8.º da Convenção Europeia dos Direitos do Homem e artigo 7.º do Pacto Internacional sobre Direitos Civis e Políticos – informação retirada de Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 736.
[69] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 30.
[70] Canotilho, Jorge J. Gomes, e Vital Moreira. *Constituição da República Portuguesa anotada, Vol. I.* 4ª edição revista e atualizada. Coimbra Editora, 2007. Página 515.
[71] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 709.

meios de as obter, quando se considere que são contrárias aos princípios de dignidade humana e Estado de Direito Democrático, tão caros ao Estado Português – artigo 1.º e 2.º CRP. É claro que, principalmente no âmbito do processo penal, sempre existirá tensão entre a descoberta da verdade e o respeito pelos direitos de todos os indivíduos, inclusive dos agentes criminosos (que são pessoas[72]). Assim, "a eficácia da Justiça é também um valor que deve ser perseguido, mas, porque numa sociedade livre os fins nunca justificam os meios, só é aceitável quando alcançada lealmente, pelo engenho e arte, nunca pela força bruta, pelo artifício ou pela mentira, que degradam quem os sofre, mas não menos quem os usa"[73] – a chamada "verdade processualmente válida" e "superioridade ética do Estado".

Este número 8 do artigo 32.º está a prever "não só a imposição de condicionamentos formais ao acesso aos meios de prova que representem uma intromissão na vida privada, como, também, a existência de restrições à valoração de provas, que devem aferir-se, conforme o exposto, pelas exigências do princípio da proporcionalidade, sempre ressalvando a ineliminável dignidade e integridade da pessoa humana"[74] – ou seja, mesmo que se recolham os meios de prova em respeito pelas regras previstas, têm de ser respeitados os princípios da adequação, proporcionalidade e proibição do excesso: no que toca aos meios de interceção de comunicações em tempo real, de modo secreto, apenas podem ser utilizados nos casos estritamente necessários, em que o meio de obtenção de prova é o único que permita a obtenção dos meios de prova, sendo necessário, por isso, averiguar da sua necessidade e adequação. Assim, "o que há de novo no n.º 8 não é a proibição do uso de meios proibidos na obtenção dos elementos de prova, mas essencialmente a utilização das provas obtidas por tais meios. Essas provas é que são nulas, nulidade que deve ser considerada em sentido forte, ou seja, como proibição absoluta da sua utilização no processo;

[72] Sobre a interessante questão, consultar: Dias, Augusto Silva. "Os criminosos são pessoas? Eficácia e garantia no combate ao crime organizado." Em *Que futuro para o direito processual penal?*, de Mário F. Monte, 687-708. Coimbra Editora, 2009.
[73] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 736.
[74] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 736.

seria intolerável que para realizar a Justiça no caso fossem utilizados elementos de prova obtidos por meios vedados pela Constituição e incriminados pela lei"[75].

Entendemos, como Jorge Canotilho e Vital Moreira, que esta "compensação" da desigualdade entre as posições da acusação e da defesa, caraterística do processo penal, era necessária, para que não restem dúvidas da posição de neutralidade e superioridade ética que o Estado deve ter, não descurando os direitos fundamentais dos indivíduos em ordem à descoberta da verdade, utilizando quaisquer meios para esse fim. Assim se consagra a proibição da instrumentalização dos direitos fundamentais dos indivíduos em relação a qualquer fim, mesmo que seja a descoberta da verdade material – pois o Estado deve respeitar as regras que ele próprio cria, tendo erigido um processo penal que respeita os princípios fundamentais da garantia da dignidade da pessoa humana e do Estado de Direito Democrático, sendo os direitos dos indivíduos limitação à sua atuação, sempre e em qualquer campo[76].

Cabe uma precisão. Quanto à nulidade consagrada no artigo 32.º n.º 8 CRP, "é absoluta no caso do direito à integridade pessoal e, relativa, nos restantes casos, devendo ter-se por *abusiva* a intromissão quando efetuada fora dos casos previstos na lei e sem intervenção judicial (artigo 32.º n.º 2 e 4), quando desnecessária ou desproporcionada ou quando aniquiladora dos próprios direitos (cfr. Artigo 18.º n.º 2 e 3)"[77].

d) *Nemo tenetur se ipsum accusare*

Normalmente definido pelo brocardo *nemo tenetur se ipsum accusare*, o princípio da não autoincriminação ou não autoinculpação significa que "ninguém pode ser coativamente

[75] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 736.
[76] Conforme se retira e conclui de Canotilho, Jorge J. Gomes, e Vital Moreira. *Constituição da República Portuguesa anotada, Vol. I.* 4ª edição revista e atualizada. Coimbra Editora, 2007. Página 516.
[77] Canotilho, Jorge J. Gomes, e Vital Moreira. *Constituição da República Portuguesa anotada, Vol. I.* 4ª edição revista e atualizada. Coimbra Editora, 2007. Página 524.

obrigado a contribuir ativamente para a sua própria condenação em processo criminal"[78 e 79], contribuindo para a sua culpabilidade[80], tendo como corolários o direito ao silêncio e o direito de não facultar meios de prova.

A Constituição da República Portuguesa não consagra expressamente o princípio contra a autoincriminação, tal como faz a Constituição Espanhola, Brasileira ou Norte-Americana. No entanto, é unânime entre a doutrina e jurisprudência que este princípio goza de proteção constitucional, enquanto princípio implícito, que decorre de outros que enformam a Lei Fundamental, tais como o princípio do processo equitativo plasmado no artigo 20.º n.º 4 CRP, decorrente do princípio de Estado de Direito Democrático – artigo 2.º CRP, as garantias plasmadas no artigo 32.º e o princípio da presunção da inocência constante do artigo 32.º n.º 2 CRP, para além de direitos como o direito à integridade pessoal e à privacidade[81].

O Tribunal Europeu dos Direitos do Homem tem entendido que o princípio quanto à não autoincriminação deriva do princípio de processo equitativo, plasmado no artigo 6.º n.º 1 da Convenção Europeia dos Direitos do Homem, tal como o direito ao silêncio – que, apesar de não serem diretamente mencionados no artigo, são considerados "*standards* internacionais que se situam no coração da noção de «processo equitativo» (*fair procedure*), tendo na sua razão de ser a ideia de proteção do acusado contra o exercício impróprio de poderes coercivos pelas autoridades, enquanto condição essencial ao acautelamento do perigo de adulteração

[78] Andrade, Manuel da Costa. "Nemo tenetur se ipsum accusare e o direito tributário ." *Boletim de Ciências Económicas da Faculdade de Direito da Universidade de Coimbra*, 2014: 385-451. Página 416.
[79] Quanto à aplicabilidade do direito à não autoincriminação no âmbito de outros ramos do Direito, consultar: Dias, Augusto Silva. "O direito à não auto-inculpação no âmbito das contra-ordenações do Código dos Valores Mobiliários." *Revista da Concorrência e Regulação*, Janeiro-Março de Ano 1, 2010: 237-265. Página 242. Silva, Maria de Fátima Reis. "O direito à não auto-incriminação." *Sub Judice n.º 40*, 2007: 59-74. Andrade, Manuel da Costa. "Nemo tenetur se ipsum accusare e o direito tributário ." *Boletim de Ciências Económicas da Faculdade de Direito da Universidade de Coimbra*, 2014: 385-451. Ramos, Vânia Costa. "Nemo tenetur se ipsum accusare e concorrência. Jurisprudência do Tribunal de Comércio de Lisboa." *Revista de Concorrência e Regulação n.º 1*, Janeiro-Março de ano 1, 2010: 175-198.
[80] Ramos, Vânia Costa. "Corpus Iuris 2000 - Imposição ao arguido de entrega de documentos para prova e nemo tenetur se ipsum accusare." *Revista do Ministério Público*, Outubro-Dezembro de 2006, ano 27: 125-149. Página 131.
[81] Como se retira e infere de Dias, Augusto Silva. "O direito à não auto-inculpação no âmbito das contra-ordenações do Código dos Valores Mobiliários." *Revista da Concorrência e Regulação*, Janeiro-Março de Ano 1, 2010: 237-265. Página 242.

da justiça e, neste sentido, à própria realização plena do espírito do artigo 6.º da Convenção"[82].

Este princípio encontra afirmação no Código de Processo Penal na afirmação do direito ao silêncio do arguido, que não o pode prejudicar – artigo 61.º n.º 1 d), e ainda nos artigos 58.º n.º 2, 132.º n.º 2 e 141.º n.º 4 – que estabelecem o direito ao silêncio que assiste ao arguido e qualquer testemunha em atos processuais determinados e que estabelecem a obrigatoriedade de informação ao arguido de que pode optar por não prestar quaisquer declarações, sem que disso possam ser retiradas consequências desfavoráveis à sua posição.

Não é de estranhar que se afirme que "o princípio *nemo tenetur se ipsum accusare* constitui pedra de toque decisiva na delimitação das fronteiras entre o processo de estrutura acusatória e as manifestações de inquisitoriedade processual"[83]. Assim é, pois, afirma a posição de sujeito processual que o arguido ocupa no processo penal, impedindo que seja tratado como um meio de prova – característico de processos inquisitórios, em que o direito ao silêncio não tinha qualquer valor: "o suspeito era obrigado a declarar contra si e a fazê-lo com verdade. A confissão do arguido, constituindo *probatio probatissima*, bastava para fundar a condenação sem admissibilidade de prova em contrário e tornava impossível o recurso"[84]. Com a transição para o modelo de estrutura acusatória e perceção do arguido como sujeito processual, a confissão deixa de ser o elemento essencial para a condenação do deste, passando a sua tentativa de obtenção a todo o custo a ser incompatível com o estatuto de sujeito do arguido, sendo necessário que se respeitem formalismos processuais para que se encontrem os meios probatórios que levarão à condenação do arguido, sem exceder os limites considerados como inultrapassáveis num Estado de Direito – a obtenção de prova através da "tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva

[82] Como se retira de Costa, Joana. "O princípio nemo tenetur na Jurisprudência do Tribunal Europeu dos Direitos do Homem." *Revista do Ministério Público n.º 128*, Outubro-Dezembro de Ano 32, 2011: 117-183. Página 118.
[83] Silva, Sandra Oliveira e. "O arguido como meio de prova contra si mesmo: considerações em torno do princípio nemo tenetur se ipsum accusare." *Revista da Faculdade de Direito da Universidade do Porto*, Ano X, 2013: 361-379. Página 364.
[84] Silva, Sandra Oliveira e. "O arguido como meio de prova contra si mesmo: considerações em torno do princípio nemo tenetur se ipsum accusare." *Revista da Faculdade de Direito da Universidade do Porto*, Ano X, 2013: 361-379. Página 364.

intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações", conforme o artigo 32.º n.º 8 CRP.

Quanto à aplicabilidade do princípio contra a autoincriminação, o Tribunal Europeu dos Direitos do Homem tem entendido que assiste a quem possua uma "posição substancialmente afetada por uma acusação de sentido equivalente ao da suspeita que oficialmente lhe é atribuída pelas autoridades"[85], relacionando-se "em primeira linha com o respeito pela vontade da pessoa do acusado em permanecer em silêncio e, embora se estenda também ao uso de poderes coercivos para obtenção de prova documental através da colaboração ativa do acusado, não abrange já a utilização, em processo penal, de elementos suscetíveis de serem obtidos do acusado através do exercício de poderes compulsivos, contando que a respetiva existência seja independente da vontade do suspeito, tais como documentos apreendidos em buscas, amostras de sangue ou de urina e tecidos corporais para testes de ADN"[86 e 87].

Costa Andrade, num esforço de redução da complexidade do que seja o princípio e direito contra a autoincriminação, entende que este apenas impede a coação para que o sujeito contribua de forma *ativa* para a sua condenação, sendo irrelevantes os seus contributos *passivos* "nomeadamente os resultantes da tolerância passiva às injunções ou intromissões das autoridades"[88] (como por exemplo as manobras de provocação artificial do vómito). Assim, pois, "do ponto de vista do atentado à dignidade pessoal do arguido convertido em instrumento da sua própria condenação, uma coisa é a recolha de provas à custa do aproveitamento e da manipulação de um arguido passivo, nas situações em que ele é

[85] Como conclui Costa, Joana. "O princípio nemo tenetur na Jurisprudência do Tribunal Europeu dos Direitos do Homem." *Revista do Ministério Público n.º 128,* Outubro-Dezembro de Ano 32, 2011: 117-183. Página 180.
[86] Costa, Joana. "O princípio nemo tenetur na Jurisprudência do Tribunal Europeu dos Direitos do Homem." *Revista do Ministério Público n.º 128,* Outubro-Dezembro de Ano 32, 2011: 117-183. Página 180.
[87] Por sua vez, indagando sobre qual o critério a adotar para a delimitação de aplicabilidade do princípio contra a autoincriminação, Sandra Oliveira e Silva "coloca as fronteiras da prerrogativa contra a autoincriminação entre a proibição de todas as formas não voluntárias de colaboração probatória do arguido e a redução do nemo tenetur à sua expressão mais nuclear de liberdade negativa de declaração (que exclui do seu âmbito todos os atos de colaboração não-verbal)". Como se retira de Silva, Sandra Oliveira e. "O arguido como meio de prova contra si mesmo: considerações em torno do princípio nemo tenetur se ipsum accusare." *Revista da Faculdade de Direito da Universidade do Porto,* Ano X, 2013: 361-379. Página 378.
[88] Andrade, Manuel da Costa. "Nemo tenetur se ipsum accusare e o direito tributário ." *Boletim de Ciências Económicas da Faculdade de Direito da Universidade de Coimbra,* 2014: 385-451. Página 416. Existem, no entanto, vozes na doutrina que invocam as dificuldades práticas de destrinça entre o que sejam as modalidades de colaboração ativa e passiva.

legitimamente tratado como objeto de prova; outra, muito diferente, é a apresentação de provas produzidas pelo arguido e, como tais, levadas à conta de ecos ou reflexos da «sua» versão dos factos, *sc.*, da «sua» vontade"[89]: no primeiro caso, a prova é produzida pelas instâncias de perseguição penal, ao passo que no segundo "a prova sempre poderá reivindicar-se da plausibilidade acrescida de aparecer no processo como projeção direta da personalidade e da «ação» do arguido"[90], sendo este instrumentalizado para obtenção de meios probatórios através da sua ação, expressão da sua personalidade e de decisão autónoma da sua vontade.

Por outro lado, o Autor entende que o *nemo tenetur* pretende impedir os casos de obtenção *coativa* de atos autoincriminatórios em que se recorre a "formas *enganosas* que comprometem igualmente a liberdade de formação e de realização da vontade"[91], considerando a corrente maioritária que se deve limitar a aplicação do princípio à autoincriminação coativa e consciente – não faltando, no entanto, vozes que propugnam pela extensão da aplicação do princípio às formas de autoincriminação obtidas mediante o engano ou erro, e por isso, atuação inconsciente. Neste ponto se inclui a utilização de meios enganosos de obtenção de prova ocultos, tal como a utilização de agentes encobertos.

Qualquer meio de ingerência nas comunicações fechadas e privadas dos indivíduos integra a categoria dos métodos ocultos de obtenção de prova – tal como as escutas telefónicas, por exemplo. É por isso necessário indagar se as informações recolhidas através destes meios devem estar, ou não, impedidas pelo princípio contra a autoincriminação, tratando-se uma atuação inconsciente por parte do sujeito investigado, que se autoincrimina com a convicção errónea de não estar a ser "escutado" ou "vigiado". Face a esta questão, consideramos que não é de estender a aplicação e limitação do *nemo tenetur* às formas autoincriminatórias recolhidas através das escutas telefónicas e outros meios equiparados (pelo artigo 189.º CPP), pois não existe qualquer coação ou elemento enganador que leve o sujeito a proferir ou escrever determinada coisa que constituam um ato de autoincriminação.

[89] Andrade, Manuel da Costa. "Nemo tenetur se ipsum accusare e o direito tributário ." *Boletim de Ciências Económicas da Faculdade de Direito da Universidade de Coimbra*, 2014: 385-451. Página 417, nota 26.
[90] Andrade, Manuel da Costa. "Nemo tenetur se ipsum accusare e o direito tributário ." *Boletim de Ciências Económicas da Faculdade de Direito da Universidade de Coimbra*, 2014: 385-451. Página 417, nota 26.
[91] Andrade, Manuel da Costa. "Nemo tenetur se ipsum accusare e o direito tributário ." *Boletim de Ciências Económicas da Faculdade de Direito da Universidade de Coimbra*, 2014: 385-451. Página 417.

Em qualquer caso, qualquer meio de ingerência nas comunicações dos indivíduos pode não revelar qualquer informação relevante para a investigação criminal, uma vez que os investigados nada disseram ou escreveram que lhe seja útil. Para além disso, não existe qualquer procedimento por parte das instâncias investigatórias que fomente o "engano" por parte do sujeito: é certo que não sabe que está a ser "vigiado", mas nem por isso se sente "tentado" a revelar informações através de conversações telefónicas, e-mail ou outras formas de comunicação intercetáveis, tal como aconteceria com a utilização de agentes encobertos – que não possuem o nível de aceitação generalizada e ponderada quanto à lesividade a nível dos direitos dos investigados como possuem as escutas telefónicas.

Por sua vez, Paulo de Sousa Mendes questiona qual será a razão de as declarações do arguido recolhidas mediante o recurso a escutas telefónicas podem ser valoradas "como prova no julgamento, enquanto prova documental"[92], entendendo que "o sistema processual penal aparenta aqui uma fragilidade axiológica, pois não reconhece ao arguido o direito de dispor daquilo que disse em conversas telefónicas ou outras que ficaram registadas por meios tecnológicos, quando se suporia que as mesmas até beneficiam de tutela reforçada, dada a proteção constitucional do segredo das comunicações e da privacidade"[93] – apenas compreendendo esta possibilidade se se entender que as declarações dirigidas a terceiros, diferentes das entidades que procedem à investigação, não estão abrangidos pelo princípio contra a autoincriminação – que, dado o exposto, nos afigura como sendo a solução mais coerente e adequada.

e) Direito à autodeterminação informacional

O direito à autodeterminação informacional está plasmado no artigo 35.º CRP[94]. Em normativos internacionais, também se encontra referência no artigo 12.º da Declaração

[92] Mendes, Paulo de Sousa. "O processo penal entre a eficácia e as garantias." Em *Direito da Investigação Criminal e da Prova*, de AA. VV., 67-80. Almedina, 2014. Página 77.
[93] Mendes, Paulo de Sousa. "O processo penal entre a eficácia e as garantias." Em *Direito da Investigação Criminal e da Prova*, de AA. VV., 67-80. Almedina, 2014. Página 77.
[94] Jorge Miranda e Rui Medeiros relembram que "não existe consenso absoluto quanto ao modelo constitucional a seguir como forma de assegurar as faculdades individuais que integram o conteúdo essencial do direito à proteção dos dados pessoais perante o uso das novas tecnologias e, em particular, da informática", sendo que, entre nós se optou pela consagração expressa do direito à proteção dos dados pessoais - Miranda, Jorge, e Rui

Universal dos Direitos do Homem, no artigo, no artigo 8.º da Convenção Europeia dos Direitos do Homem e no artigo 17.º do Pacto Internacional relativo aos direitos civis e políticos. Apesar de não ser o foco direto da presente investigação, não podemos furtar-nos a uma breve análise a este direito devido à sua importância no domínio das comunicações, num contexto de crescente informatização de dados e possibilidades de acesso aos dados atinentes às comunicações, como sejam aos dados pessoais dos indivíduos, armazenados na *rede* e nas empresas de telecomunicações – sendo inclusivamente a venda entre empresas desses mesmos dados negócio bastante rentável nos dias de hoje[95].

Jorge Canotilho e Vital Moreira entendem que o artigo 35.º CRP, que consagra a proteção contra o tratamento informático de dados pessoais, se opera fundamentalmente em três direitos – "direito de acesso das pessoas aos registos informáticos para conhecimento dos seus dados pessoais neles constantes (n.º 1), bem como a retificação e complementação dos mesmos", "direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros dos dados pessoais informatizados e direito à sua não interconexão (n.º 4)", "direito ao não tratamento informático de certos tipos de dados pessoais (n.º 3); "proibição de número nacional único (n.º 5) funciona como garantia daqueles direitos, dificultando o tratamento informático de dados pessoais e a sua interconexão, que seria facilitada com um identificador numérico comum"[96].

Devido à "pegada eletrónica" que as novas tecnologias permitem seguir, cada vez são "mais importantes as garantias contra o tratamento e a utilização abusiva de dados pessoais informatizados"[97]. Assim, o direito à autodeterminação informativa "está longe de ser apenas uma garantia do direito à intimidade da vida privada, constitui um verdadeiro feixe de prerrogativas que asseguram que cada um de nós decida até onde vai a sombra que deseja que paire sobre as informações que lhe respeitam. É uma liberdade, um poder de dispor das

Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 783.

[95] Como se pode ver na reportagem de Raquel Marinho e produção de Cláudia Araújo, de fevereiro de 2016, disponível em http://expresso.sapo.pt/multimedia/video/2016-02-21-Identidade-a-venda-os-dados-pessoais-na-internet, acedida e consultada a 05-10-2016.

[96] Canotilho, Jorge J. Gomes, e Vital Moreira. *Constituição da República Portuguesa anotada, Vol. I.* 4ª edição revista e atualizada. Coimbra Editora, 2007. Página 55.

[97] Canotilho, Jorge J. Gomes, e Vital Moreira. *Constituição da República Portuguesa anotada, Vol. I.* 4ª edição revista e atualizada. Coimbra Editora, 2007. Página 550.

suas informações pessoais, um poder de controlo através de cujo exercício se permitirá que cada indivíduo determine o que podem os outros, a cada momento, saber a seu respeito"[98]. Catarina Sarmento e Castro concretiza este direito em várias dimensões: "direito ao esquecimento", impondo um período máximo de conservação dos dados pessoais; "direito à curiosidade", que assegura aos indivíduos o direito se assegurar quem tem conservados os seus dados pessoais, de forma direta ou indireta; "direito de informação", que garante ao indivíduo o direito de saber quais as finalidades do tratamento de dados, bem como a identidade do responsável pelo mesmo; sendo complementados pelo "direito de acesso aos dados pessoais" e o de obter "retificação", "atualização" e "clarificação" dos mesmos. Para além destes direitos, a Autora faz referência ao "direito ao não tratamento de dados sensíveis", nomeadamente de informações relativas à saúde e genética do titular dos dados, vida sexual, convicções filosóficas ou políticas, etc.

Quanto a esta temática, estão em vigor, em Portugal, a Lei de Proteção de Dados Pessoais, Lei n.º 67/98, de 26 de Outubro, A Lei de Proteção Dados Pessoais e Privacidade nas Telecomunicações, de Lei n.º 41/2004, de 18 de Agosto, a Lei que regula a conservação de dados gerados ou tratados no contexto de serviços de comunicações eletrónicas, Lei n.º 32/2008, de 17 de Julho – sem esquecer da Lei do Cibercrime, Lei 109/2009, que consagra meios de obtenção e de prova que contendem com dados informáticos.

O conceito de dados pessoais é um conceito abrangente, que encontra definição na Lei de Proteção de Dados Pessoais, Lei n.º 67/98, de 26 de Outubro, no seu artigo 3.º: dados pessoais são "qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social". Infra se analisará a "conservação de dados gerados ou tratados no contexto de serviços de comunicações eletrónicas" previstos na Lei 32/2008[99].

[98] Castro, Catarina Sarmento e. "Protecção de dados pessoais na Internet." *Revista Sub Judice*, Setembro de n.º 35, 2006: 11-29. Página 16.
[99] Nomeadamente no Capítulo III, ponto 5 b) e c).

Capítulo II – A intromissão nas comunicações fechadas

> "A sociedade da informação trouxe no ventre um surto de novos serviços e cuja tecnologia nos vislumbram e fazem a delícia dos mais novos e, no reverso da medalha, vieram à baila alguns dos ataques mais letais à nossa privacidade e intimidade."[100]
>
> Benjamim da Silva Rodrigues

1. Considerações introdutórias

Parece estar demonstrada a importância da comunicação para os indivíduos para a sua realização, expressão última do direito à palavra e à reserva da intimidade da sua privada, como meio para a concretização do Homem como ser-pessoa, um "animal político", que mais do que ser social que vive em comunidade, procura construir uma sociedade – em que "o ato comunicacional é afirmação de abertura ao outro", o que supõe que o "«eu», para se desenvolver harmoniosamente, crie espaços onde o «outro» só pode penetrar quando aquele, o «eu», em atitude de auto-realização, o permita" [101].

Quando comunicam, e sobretudo quando pretendem que a comunicação se mantenha dentro de um círculo de pessoas determinadas, *fechada*, os indivíduos confiam que apenas os interlocutores da conversação poderão ter acesso às palavras ditas ou escritas, sem que exista qualquer gravação ou registo que não autorizaram ou pretendem, nomeadamente por terceiros.

Concordamos com Garcia Marques e Lourenço Martins quando afirmam que no âmbito da vida privada e das liberdades pessoais é onde se revelam os maiores afrontamentos entre o poder político e a sociedade civil, devido ao desenvolvimento da informática e à

[100] Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 158.
[101] Costa, José Francisco de Faria. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998. Página 70.

possível utilização abusiva da mesma[102]. Assim é, pois se, por um lado, "pode dizer-se que as novas tecnologias, em geral, e a informática, em especial, proporcionam ao homem uma capacidade nova para a expressão da sua vontade e, portanto, para o exercício da sua liberdade", por outro, "o recurso aos sofisticados instrumentos das modernas tecnologias faz com que aumentem os riscos de violação das liberdades individuais, mormente da intimidade da vida privada, gerando também um acréscimo de perigos de discriminação em função de circunstâncias estreitamente ligadas à personalidade, às crenças, ideologias ou modo de vida dos cidadãos"[103].

Assim, face à consagração de direitos fundamentais como o direito à reserva da intimidade privada, o direito à palavra e a inviolabilidade das comunicações (principalmente), o Direito Penal não pôde ficar indiferente às possíveis violações que os direitos dos sujeitos podem sofrer, tendo sido chamado a tipificar como crime alguns comportamentos que violam a vida privada dos indivíduos. Foram consagrados como ilícitos criminais a "violação de domicílio ou perturbação da vida privada" – artigo 190.º CP[104], a "introdução em lugar vedado ao público" – artigo 191.º CP[105], a "devassa por meio de informática" – artigo 193.º CP, a "violação de correspondência ou telecomunicações" – artigo 194.º CP, e a utilização de "instrumentos de escuta telefónica" – artigo 276.º CP.

[102] Marques, Garcia, e Lourenço Martins. *Direito da Informática.* Coimbra: Almedina, 2000. Página 99.
[103] Marques, Garcia, e Lourenço Martins. *Direito da Informática.* Coimbra: Almedina, 2000. Página 99.
[104] Conforme Paulo Pinto de Albuquerque, o "bem jurídico protegido pelo crime de violação de domicílio é a privacidade de outra pessoa na sua vertente da privacidade do lar, isto é, de uma esfera privada espacial". O bem jurídico protegido pelo número 2 deste artigo é a "paz e o sossego de outra pessoa, ainda que reportados à paz e ao sossego gozados no espaço físico da habitação" – como se retira de Albuquerque, Paulo Pinto de. *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* Universidade Católica Portuguesa, 2008. Página 512.
[105] Como ensina Paulo Pinto de Albuquerque, a norma protege três bens jurídicos distintos: "por um lado, a privacidade de outra pessoa num espaço físico circundante da habitação ("pátios, jardins ou espaços verdes anexos à habitação"); por outro lado, a funcionalidade de determinados serviços ("lugar vedado e destinado a serviço ou a empresa públicos, a serviço de transporte ou ao exercício de profissões ou atividades"); por outro ainda, o direito à propriedade ("barcos ou outros meios de transporte", "outro lugar vedado e não livremente acessível")" – conforme se retira de Albuquerque, Paulo Pinto de. *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* Universidade Católica Portuguesa, 2008. Página 517.

2. Os artigos 194.º e 276.º do Código Penal

Quanto ao foco da presente investigação, as comunicações realizadas através das Internet, apesar de neste ponto analisarmos a questão da sua intromissão fora do quadro da investigação criminal (pelo menos, a que respeite os formalismos legais), tem grande importância o ilícito criminal tipificado como "violação de correspondência ou de telecomunicações", constante do artigo 194.º CP[106].

A privacidade das comunicações à distância é considerada como um bem jurídico que deve ser protegido pelo Estado, tratando-se a intromissão no conteúdo de correspondência ou da telecomunicação de terceiros um crime de "indiscrição e devassa, punindo, a par de atos de intromissão arbitrária, condutas de divulgação arbitrária"[107]. Este tipo legal de crime visa proteger a confiança nas comunicações, sendo punidos os funcionários[108] das empresas que as permitem se o cometerem no exercício de funções públicas, conforme o disposto no artigo 384.º CP[109], que consagra um crime específico impróprio[110], sendo, neste caso, o bem

[106] Dispõe o artigo 194.º CP: "1 - Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.
2 - Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento.
3 - Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias".

[107] Garcia, Miguez, e Castela Rio. *Código Penal (parte geral e especial) com notas e comentários.* Almedina, 2014. Página 798.

[108] O conceito de funcionário encontra-se plasmado no artigo 386.º CP. Paulo Pinto de Albuquerque esclarece que o "funcionário civil é o agente administrativo profissional submetido ao regime da função pública" e o "agente administrativo é a pessoa que, por qualquer título, exerce atividade ao serviço das pessoas coletivas de direito público, sob direção dos respetivos órgãos" – como se retira de Albuquerque, Paulo Pinto de. *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* Universidade Católica Portuguesa, 2008. Página 914. Para Faria Costa, esta definição do conceito de "funcionário" operada pelo artigo 386.º CP trata-se de um "alargamento da equiparação a funcionário que, em alguns casos, não tem, a nossos olhos, qualquer ligação substancial com o conceito matricial de funcionário que o direito público nos oferece", não sendo este desvio concetual fundado em razões substanciais legitimas. Sobre este ponto, consultar: Costa, José Francisco de Faria. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998. Página 91.

[109] Assim é, segundo Faria Costa, pois "o Estado é chamado a proteger a comunicação fechada, punindo não só as violações que o cidadão comum comete relativamente aos valores que ela esconde, mas também punindo os seus servidores, os funcionários, que a não defendem segundo as regras previamente estabelecidas" – como se retira de Costa, José Francisco de Faria. Direito Penal da Comunicação. Alguns escritos. Coimbra Editora, 1998. Página 100.

[110] Aquele em que a qualidade do agente apenas determina uma agravação da pena, por oposição aos crimes específicos próprios, que são aqueles em que a qualidade do agente é que justifica a criação autónoma do tipo.

jurídico protegido ainda a "integridade do exercício das funções públicas pelo funcionário"[111].

Quanto ao número 1 do artigo 194.º CP, que se refere à ingerência na correspondência, é entendimento generalizado que "a encomenda, carta ou qualquer outro escrito há-de encontrar-se fechado ao tempo da ação e não deve ser dirigido ao agente"[112] que a abrir *ou* tomar conhecimento do seu conteúdo, bastando o ato de "abrir" para ser consumado o crime – mesmo que o agente não tenha acesso ao conteúdo.

Quanto à intromissão no conteúdo das telecomunicações, aspeto que mais importa assinalar na presente investigação, encontra-se prevista no número 2 do artigo 194.º CP, e "trata-se da apreensão em tempo real do conteúdo de uma comunicação em curso, mas reservada", sendo exemplo mais vulgar a interceção telefónica, "consistente na captação de comunicações que se desenvolvem entre terceiros, realizada de modo a não impedir que a mesma prossiga e sem que os interlocutores, ou pelo menos algum deles, se deem conta da intromissão" [113] – procede-se assim em segredo, visando a continuação da comunicação de modo a poder intercetar-se o seu conteúdo, que também pode ocorrer com e-mails e outras comunicações escritas "transmitidas de computador a computador, desde que ligados pela internet, ou de computador aos aparelhos celulares, ou vice-versa" [114].

Conforme Paulo Pinto de Albuquerque, para o preenchimento do tipo objetivo deste ilícito apenas relevam os meios de telecomunicação "entre pessoas determinadas e não os meios de telecomunicação acessíveis ao público em geral ou aos subscritores de um serviço pago", estando por isso incluídos "o telefone, o telegrama, o telex, o telefax, a telefoto, o

[111] Albuquerque, Paulo Pinto de. *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* Universidade Católica Portuguesa, 2008. Página 909.
[112] Garcia, Miguez, e Castela Rio. *Código Penal (parte geral e especial) com notas e comentários.* Almedina, 2014. Página 797.
[113] Garcia, Miguez, e Castela Rio. *Código Penal (parte geral e especial) com notas e comentários.* Almedina, 2014. Página 798.
[114] Garcia, Miguez, e Castela Rio. *Código Penal (parte geral e especial) com notas e comentários.* Almedina, 2014. Página 798.

correio eletrónico" – estando excluídos a "rádio, a televisão e o teletexto" [115], revelando assim o caráter eminentemente privado do conteúdo das conversações entre os indivíduos.

O legislador tipificou ainda como crime, no âmbito do Capítulo III do Código Penal, relativo a crimes de perigo comum, os "instrumentos de escuta telefónica" – artigo 276.º CP[116]. Neste caso, há antecipação da proteção penal dos bens jurídicos de reserva da intimidade da vida privada e o segredo das comunicações e telecomunicações – "punindo a mera disponibilidade fática sobre objetos que podem servir para cometer crimes" contra aqueles[117], tendo este normativo surgido em virtude do "recente desenvolvimento da tecnologia no domínio da interceção dos meios de comunicação"[118]. Com a tipificação deste ilícito criminal como um crime de perigo abstrato, não está em causa "o tomar conhecimento efetivo de conversas telefónicas alheias, ou do conteúdo de correspondência fechada que não é dirigida ao agente, mas sim a conduta suscetível de vir a lesar a privacidade ou o segredo a que cada um tem direito no âmbito deste tipo de comunicações"[119].

3. O artigo 193.º do Código Penal

Fruto da evolução tecnológica e do surgimento da criminalidade informática, o legislador penal dispôs-se a regular a "devassa por meio de informática", no artigo 193.º CP[120].

---

[115] Como se retira de Albuquerque, Paulo Pinto de. *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* Universidade Católica Portuguesa, 2008. Página 527.

[116] Dispõe o artigo 276.º CP (Instrumentos de escuta telefónica): "Quem importar, fabricar, guardar, comprar, vender, ceder ou adquirir a qualquer título, transportar, distribuir ou detiver instrumento ou aparelhagem especificamente destinados à montagem de escuta telefónica, ou à violação de correspondência ou de telecomunicações, fora das condições legais ou em contrário das prescrições da autoridade competente, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias".

[117] Albuquerque, Paulo Pinto de. *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* Universidade Católica Portuguesa, 2008. Página 713.

[118] Como se retira de Gonçalves, Manuel Lopes Maia. *Código Penal Português - Anotado e Comentado - Legislação complementar.* 14. Almedina, 2001. Página 827.

[119] Assim entende Paula Ribeiro de Faria em Dias, Figueiredo. *Comentário Conimbricense ao Código Penal, Parte Especial.* Vol. Tomo II. Coimbra Editora, 1999. Página 904.

[120] Dispõe o artigo 193.º CP que: "1 - Quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias. 2 - A tentativa é punível".

Para o preenchimento deste tipo legal de crime é necessário que o agente crie, mantenha ou utilize algum ficheiro automatizado de que constem dados referentes a alguém, ou que possam levar a essa identificação, referentes a "convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada ou a origem étnica"[121]. O que revela não é "propriamente uma violação da privacidade ou do segredo, não obstante a sua posição sistemática, mas reforça a interdição do tratamento informático de um conjunto de dados pessoais contra a vontade do respetivo titular"[122].

Assim, com a tipificação deste tipo legal de crime o legislador demonstrou a sua preocupação com o tratamento informático de dados dos indivíduos, fruto da evolução tecnológica com que tem sido confrontado, não visando por isso a proteção da privacidade ou segredo, o que deixa a descoberto a fragilidade da própria epígrafe do artigo, que se dirige à "devassa por meio da informática": parece que essa devassa opera relativamente à privacidade dos indivíduos feita através da informática, não e não com o tratamento informatizado de dados relacionados com diversas esferas da vida dos indivíduos – que é precisamente o objeto do normativo.

João Barbosa de Macedo, já em 2009, entendia que "esta disposição deverá desaparecer em breve do Código Penal"[123]: considerava que devia constar de lei extravagante, nomeadamente da Lei de Proteção de Dados Pessoais, por razões de coerência. Estava enganado: ainda hoje, 8 anos passados, o artigo 193.º permanece no Código Penal. Este Autor, já em 2009, considerava que a Lei de Proteção de Dados Pessoais já continha disposições que visassem a criminalização de condutas que desviassem ou utilizassem dados pessoais, nomeadamente no seu artigo 43.º n.º 1 c): "É punido com prisão até um ano ou multa até 120 dias quem intencionalmente desviar ou utilizar dados pessoais, de forma incompatível com a finalidade determinante da recolha ou com o instrumento de legalização". Assim, entendia que o artigo 193.º CP se encontrava, já em 2009, note-se,

[121] Garcia, Miguez, e Castela Rio. *Código Penal (parte geral e especial) com notas e comentários.* Almedina, 2014. Página 795.
[122] Garcia, Miguez, e Castela Rio. *Código Penal (parte geral e especial) com notas e comentários.* Almedina, 2014. Página 796.
[123] Macedo, João Barbosa de. "Algumas considerações acerca dos crimes informáticos em Portugal." Em *Direito Penal hoje, desafios e respostas*, de Manuel da Costa Andrade e Rita Castanheira Neves, 221-262. Coimbra Editora, 2009. Página 256.

tacitamente revogado. Este é o primeiro ponto a assinalar de confusão do legislador no que toca à informática.

4. O artigo 7.º da Lei do Cibercrime

A Lei do Cibercrime, Lei 109/2009, consagra, no seu artigo 7.º, o crime de "interceção ilegítima" em sistemas informáticos[124].

Conforme Pedro Venâncio, neste tipo legal de crime o "bem jurídico protegido é a segurança e a privacidade das comunicações eletrónicas, havendo, por isso, um interesse do Estado em agir criminalmente"[125], protegendo os cidadãos de intromissões arbitrárias por qualquer pessoa nos sistemas informáticos que detém transmitem dados e informações particulares relativos à sua pessoa – que, com o desenvolvimento das tecnologias e a sua massiva utilização, podem ser relativos a quaisquer coisas: dados de contas bancárias e respetivos códigos de acesso, e-mail pessoal e profissional, contas de utilizador de sites, localização geográfica, etc. Este tipo legal de crime é aplicável "a todas as formas de transferência eletrónica de dados, quer se trate de uma transferência por telefone, fax, correio eletrónico ou ficheiro" [126], quando se trate de transmissões privadas, sendo esta "a natureza de comunicação na relação entre os sujeitos e não a natureza dos dados transmitidos ou utilizados" [127].

Pedro Dias Venâncio considera que o tipo legal do artigo 7.º da Lei do Cibercrime encontra paralelo no artigo 194.º do Código Penal: "De facto, tem-se entendido que o crime

[124] Dispõe o artigo 7.º da Lei do Cibercrime que: "1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa. 2 - A tentativa é punível. 3 - Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no mesmo número".
[125] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 67.
[126] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 68.
[127] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 68.

de violação de correspondência ou de telecomunicações é diretamente aplicável à correspondência eletrónica – via "e-mail" ou "Voip" -, que é modernamente perfeitamente equiparável à correspondência fechada ou às telecomunicações convencionais, sendo mesmo possível encontrar alguns pontos de contacto entre este crime e os crimes informáticos em sentido estrito"[128]. Impõe-se por isso a questão de saber se o artigo 194.º CP não será absorvido pelo 7.º LC, no que toca as comunicações eletrónicas. Este Autor considera que "embora possa existir sobreposição quanto à interceção da mensagem escrita ou da comunicação áudio ou vídeo em ambiente digital, já não haverá quando se trata da interceção de transmissão de dados informáticos de natureza diversa"[129], uma vez que o conceito de "dados informáticos" para a Lei do Cibercrime é mais amplo do que o conceito entendido sob a perspetiva do 194.º CP.

Pedro Dias Venâncio conclui assim que "se no crime do artigo 194.º CP parece prevalecer a proteção da privacidade dos dados em função da sua natureza pessoal ou confidencial, no artigo 7.º LC prevalece a proteção da privacidade e idoneidade do meio eletrónico, na lógica de reforço da confiança e segurança jurídica da Sociedade da Informação"[130].

Parece ser este mais um nódulo em que o legislador português introduziu um elemento de confusão no que toca à tipificação de crimes relacionados com o mundo informático e digital, que no essencial se sobrepõem quanto à "interceção da mensagem escrita ou da comunicação áudio ou vídeo em ambiente digital", existindo dois tipos legais que se destinam à responsabilização criminal da mesma conduta, com penas diversas, uma substancialmente mais gravosa que a outra: o artigo 7.º da LC pune com "com pena de prisão até 3 anos ou com pena de multa", enquanto que o artigo 194.º CP com "pena de prisão até 1 ano ou com pena de multa até 240 dias".

[128] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 68.
[129] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 68.
[130] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 68.

5. Disposições processuais

No âmbito do Direito Processual Penal, é evidente a importância e utilidade que a monitorização de comunicações fechadas dos indivíduos têm no contexto da investigação criminal: comunicando com alguém, e pretendendo-se que a comunicação permaneça secreta e adstrita ao círculo de destinatários definido pelo interlocutor, pode confidenciar-se qualquer detalhe sobre a prática criminalmente ilícita, seja sobre a identidade do(s) agente(s), planos de continuação da atividade, identidade da vítima ou plano de execução, podendo qualquer indivíduo revelar mais do que intencionava, e a quem não pretendia, devido à falta de consciência de estar a ser "escutado". Principalmente "perante fenómenos de criminalidade organizada e altamente complexa, onde os tradicionais métodos de recolha de prova apresentam uma dúbia eficácia"[131], há muito tempo que as escutas telefónicas se configuram como um meio de obtenção de prova importantíssimo[132], dirigindo-se à interceção de comunicações em tempo real entre os indivíduos, de modo a recolher para o processo meios de prova, estando o seu regime consagrado no artigo 187.º e seguintes do CPP – sem esquecer que, entre nós, as escutas telefónicas se inserem no quadro de uma investigação e respetivo processo em curso, em conformidade com o artigo 34.º n.º 4 da CRP, não podendo ser realizadas a título preventivo[133].

As escutas telefónicas dependem de vários pressupostos materiais para que possam ser realizadas[134], nomeadamente: é necessário que sejam autorizadas pelo Juiz de Instrução Criminal, mediante requerimento do Ministério Público e apenas durante a fase de inquérito, estando "sujeitas a um período temporalmente limitado"[135], sendo "indispensáveis para a

---

[131] Rodrigues, Cláudio Lima. "Dos pressupostos materiais de autorização de uma escuta telefónica." *verbojuridico.net.* Editado por Verbo Jurídico. Fevereiro de 2013. http://www.verbojuridico.net/ficheiros/doutrina/ppenal/claudiolimarodrigues_autorizacaoescutatelefonica.pdf (acedido em 27 de Dezembro de 2016). Página 9.

[132] Tendo aparecido as escutas telefónicas sido consagradas como meio de obtenção de prova através do Decreto-Lei n.º 78/87, que revogou o Código de Processo Penal de 1929 e instituiu o Código de Processo Penal de 1987.

[133] Quanto à questão do direito penal preventivo no quadro de uma sociedade de risco, consultar Loureiro, Flávia Noversa. "A (i)mutabilidade do paradigma processual penal respeitante aos direitos fundamentais em pleno século XXI." Em *Que futuro para o Direito Processual Penal?*, de Mário F. Monte, 269-289. Coimbra Editora, 2009.

[134] Uma análise mais aprofundada será realizada infra.

[135] Rodrigues, Cláudio Lima. "Dos pressupostos materiais de autorização de uma escuta telefónica." *verbojuridico.net.* Editado por Verbo Jurídico. Fevereiro de 2013.

descoberta da verdade" ou nos casos em que "a prova seria, de outra forma, impossível ou muito difícil de obter", quanto aos crimes pertencentes ao catálogo constante no artigo 187.º CPP. Assim, com as escutas, podem ser recolhidas informações valiosas para a investigação criminal e garantia de eficácia da mesma, ou até mesmo na descoberta de informações inesperadas sobre as situações não inicialmente investigadas – conhecimentos válidos, desde que verificados os requisitos de admissibilidade das escutas, que poderão servir como meio de prova noutro processo judicial, conforme o disposto no artigo 187.º n.º 6 CPP[136].

Face aos desenvolvimentos tecnológicos a que se tem assistido, no domínio da informação e da comunicação, têm surgido fenómenos de criminalidade informática[137] – que o legislador consagrou na Lei do Cibercrime, Lei 109/2009 de 15 de Setembro, que contém disposições de direito penal material quanto a esta forma de criminalidade, e também disposições adjetivas, consagrando meios de obtenção de prova como a "preservação expedita de dados", a "revelação expedita de dados de tráfego", a "injunção para apresentação ou concessão do acesso a dados", a "pesquisa de dados informáticos", a "apreensão de dados informáticos" e "apreensão de correio eletrónico e registos de comunicações de natureza semelhante" – todos aplicáveis em relação aos tipos legais de crime estabelecidos no normativo, a todos os demais crimes cometidos por meio de utilização da informática ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico (artigo 11.º da Lei do Cibercrime); e ainda a "interceção de comunicações" e as "ações encobertas" – que só são aplicáveis aos tipos materiais de crime previstos na Lei

http://www.verbojuridico.net/ficheiros/doutrina/ppenal/claudiolimarodrigues_autorizacaoescutatelefonica.pdf (acedido em 27 de Dezembro de 2016). Página 5.

[136] Quanto à problemática dos conhecimentos fortuitos, embora ultrapassada com a reforma de 2007 que consagrou a sua admissibilidade nos termos do artigo 187.º n.º 6 CPP, consultar, entre outros, Monte, Mário Ferreira. "Escutas telefónicas." Em *III Congresso de Processo Penal - Memórias*, de AA. VV., 163-195. Almedina, 2010. Página 164 e seguintes. Aguilar, Francisco. *Dos conhecimentos fortuitos obtidos através de escutas telefónicas. Contributo para o seu estudo nos ordenamentos jurídicos alemão e português.* Coimbra: Almedina, 2004. e Valente, Manuel. *Conhecimentos fortuitos. A busca de um equilíbrio apuleiano.* Coimbra: Almedina, 2006.

[137] Consideramos, tal como Pedro Venâncio, que a criminalidade informática pode ser entendida em sentido amplo e em sentido estrito: a primeira "englobará toda a panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais do que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios"; ao passo que a segunda "abarcará apenas aqueles crimes em que o elemento digital surge como parte integradora do tipo legal ou mesmo como seu objeto de proteção" – como se retira de Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada*. Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 17.

do Cibercrime. Podemos concluir, tal como faz Pedro Venâncio[138], que os meios de obtenção de prova consagrados na Lei do Cibercrime, nomeadamente "apreensão de correio eletrónico e registos de comunicações de natureza semelhante", a "interceção de comunicações" e as "ações encobertas" são novas aplicações para os instrumentos tradicionais do processo penal, no âmbito do ambiente digital.

Coloca-se assim a questão de saber se serão ainda as escutas telefónicas, regime tradicional para a interceção de comunicações em tempo real (fundamental numa época em que o telefone – analógico – era o principal meio de comunicação[139]), o indicado para a ingerência nas "novas" comunicações, que são realizadas através de meios tao diversos entre si, e em relação ao meio para que as escutas telefónicas foram pensadas, o telefone fixo. O problema coloca-se devido à afirmação das comunicações eletrónicas – que se processam através de suportes digitais e da Internet, e mesmo que faladas – através do *Voice over IP*, podem inclusivamente ser encriptadas. *Skype, WhatsApp, Facebook Messenger, Outlook e Gmail* têm-se afirmado como indispensáveis para comunicação nas sociedades atuais, sendo inegável a proliferação de diferentes meios de comunicação "à distância", através da *rede das redes*.

A nível normativo, esta questão tem suporte no artigo 189.º n.º 1 CPP, que consagra que o regime das escutas telefónicas é "correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes". O que não se pode esquecer é que a Lei do Cibercrime consagra normas processuais quanto

[138] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 91.

[139] Tal como relembra Paulo Dá Mesquita, o "dispositivo *telefone* compreende uma realidade abrangente do processamento de comunicação que inclui **telefones analógicos** (que transportam apenas transmissões de voz e frequências de sinalização) e **telefones digitais**", sendo que esta "compreende a utilização da eletrónica digital no fornecimento de serviços telefónicos digitais em que os telefones enviam uma camada para a transmissão de dados, camada de dados que permite o tráfego de informações sobre a ligação em curso ou enviar informações para interagir com uma *PABX* (*Private Automatic Branch Exchange*) que permite efetuar ligações entre telefones internos sem intervenção manual, ou ainda telefonar e receber telefonemas da rede externa (geralmente pública)". Este Autor nota que "mesmo os telefones analógicos podem utilizar a tecnologia *VoIP*, desde que a *PABX* a que estão ligados disponha de conversores (*gateways*) apropriados" (negrito nosso) – como se retira de Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 103, nota de rodapé número 41.

à apreensão de correio eletrónico (que tal como visto sumariamente, pela ação do artigo 11.º, se aplica a qualquer crime, previsto ou não na Lei do Cibercrime, desde que cometido por recurso a sistemas informáticos ou perante os quais seja necessária o recurso a prova eletrónica) e a interceção de comunicações eletrónicas, mas este restrito ao catálogo de crimes previsto na Lei do Cibercrime – artigos 17.º e 18.º da Lei do Cibercrime, respetivamente. Qual é, então, o regime para a apreensão de correio eletrónico e registos de natureza semelhante – o Código de Processo Penal, por força do artigo 189.º n.º 1, ou a Lei do Cibercrime, por força do artigo 17.º? Ou ambos… E quanto à interceção de comunicações de voz realizadas através da Internet e mensagens de texto enviadas através de chats e de forma instantânea?

As questões enunciadas não são de supérflua importância, pois ao determinar qual o regime vigente na matéria de obtenção de prova através da apreensão de correio eletrónico e através "interceção" de comunicações, o legislador impõe formalismos e realiza uma ponderação *ex ante* dos impactos do meio de obtenção de prova e quais os procedimentos a adotar para que a obtenção de prova seja válida. Numa investigação criminal enquadrada num Estado de Direito não se pode admitir a utilização de meios de obtenção de prova que não estejam consagrados na lei, ou cujos limites não sejam respeitados. Assim, em respeito pelo princípio da legalidade, não podem ser utilizadas as provas obtidas através da utilização de "escutas telefónicas" ilegais (artigo 190.º CPP), bem como a prova obtida através da intromissão na vida privada, domicílio, correspondência ou nas telecomunicações, sem que esteva previsto na Lei ou que o titular preste o seu consentimento – artigo 126.º n.º 3 CPP. E tendo sempre em mente que "o que é tecnicamente possível não é, só por si e sem mais, legítimo"[140], para que se aplique um meio de obtenção de prova numa investigação criminal é necessário que o legislador tenha realizado a ponderação necessária à realidade e adequação entre o meio de obtenção de prova e o meio de comunicação utilizado, e consagrar essa solução.

Resta saber que meios de "ingerência", "vigilância" ou "monitorização" das comunicações são, e devem ser, admitidos no ordenamento jurídico português.

[140] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 150.

Capítulo III – Os meios de obtenção de prova no Direito Português

> "À oscilação social e cultural da comunidade que, temporalmente determinada, busca agora um conjunto diferente de garantias e prestações por parte do Estado, tem hoje o Direito, no caso, o direito processual penal, de responder com habilidade e sabedoria, por forma a reequilibrar os pratos desta balança, em respeito, obrigatoriamente, pelas normas constitucionais, sobretudo pela que impõe o princípio da proporcionalidade nesta matéria, mas correspondendo às aspirações, legítimas enquanto tais, dos cidadãos da comunidade."
>
> Flávia Noversa Loureiro[141]

1. Considerações introdutórias

Apesar de haver quem advogue que as distinções concetuais apenas "desviam a discussão sobre o verdadeiro Direito"[142], consideramos que são precisamente os conceitos a base de qualquer dogmática, delimitando os temas e permitindo a sua compreensão, bem como a correta apreensão da "função processual"[143] de qualquer instituto. Assim, mais uma vez realçamos a importância que julgamos que tais distinções possuem – neste caso, relativas à definição de meios prova e meios de obtenção de prova.

---

[141] Loureiro, Flávia Noversa. "A (i)mutabilidade do paradigma processual penal respeitante aos direitos fundamentais em pleno século XXI." Em *Que futuro para o Direito Processual Penal?*, de Mário F. Monte, 269-289. Coimbra Editora, 2009. Página 275.

[142] Aguilar, Francisco. "Notas reflexivas sobre o regime das escutas telefónicas no Código de processo penal português." *O Direito*, 2016 III, ano 148: 559-583. Página 559. Este Autor considera que "os conceitos, no quadro do Direito, não devem passar de meros instrumentos do diálogo científico, não devendo, por conseguinte, em caso algum, ser utilizados para fundamentar uma decisão". Consideramos que os conceitos, precisamente por serem instrumentais em relação a qualquer discussão jurídica que se encete, são determinantes para a solução a adotar, em qualquer caso: sempre porque serão os conceitos que determinarão as questões a discutir e analisar, sendo a qualificação jurídica fundamental no mundo do Direito.

[143] Nesse sentido entendem Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014. Página 785.

Os meios de prova caracterizam-se pela "aptidão de serem, por si próprios, fonte de conhecimento, ao contrário dos meios de produção de prova que são instrumentos para atingir aqueles meios ou elementos de prova"[144] – consubstanciando os primeiros o conhecimento direto e próprio dos factos a provar em juízo, enquanto que os segundos são os métodos utilizados para os recolher para o processo criminal.

A função primordial da prova é a demonstração em juízo da realidade dos factos[145] – eliminando o arbítrio das decisões judiciais e estabelecendo a justiça processual, sendo balizada pela exclusão dos meios de prova e da sua obtenção que sejam ilícitos, por não toleráveis num Estado de Direito, e ainda pela obrigatoriedade da fundamentação judicial que justifique a utilização e valoração do material probatório utilizado[146].

O direito processual penal português possui uma estrutura acusatória integrada pelo princípio da investigação, que se traduz na característica da entidade que acusa (o Ministério Público – artigos 53.º e 262.º CPP) ser distinta da que irá julgar (o juiz em tribunal singular, coletivo ou de júri – artigo 13.º, 14.º e 16.º CPP), cabendo à primeira a recolha de prova suficiente para acusar pela prática de factos penalmente ilícitos, tendo tribunal o dever de "esclarecer e instruir autonomamente – isto é, independentemente das contribuições da acusação e da defesa – o "facto" sujeito a julgamento, criando ele próprio as bases necessárias à sua decisão"[147].

O Estado tem a tarefa fundamental de "garantir os direitos e liberdades fundamentais"[148], devendo reprimir e dissuadir os indivíduos da prática criminosa que lesa

---

[144] Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado*. 1ª. Almedina, 2014. Página 785.

[145] À falta de consagração da definição de prova na legislação penal, é necessário recorrer ao Código Civil, que a define no seu artigo 341.º: "As provas têm por função a demonstração da realidade dos factos".

[146] Como se infere de Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 67.

[147] Dias, Figueiredo. "Direito Processual Penal - Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por Maria João Antunes, Assistente da Faculdade de Direito da Universidade de Coimbra." Coimbra: Secção de Textos da Faculdade de Direito da Universidade de Coimbra, 1998/1999. Página 51.

[148] Conforme o artigo 9.º da Constituição da República Portuguesa: "São tarefas fundamentais do Estado:
a) Garantir a independência nacional e criar as condições políticas, económicas, sociais e culturais que a promovam;
b) Garantir os direitos e liberdades fundamentais e o respeito pelos princípios do Estado de direito democrático;

bens jurídicos ascendidos à categoria de fundamentais para a sociedade, cuja violação é consagrada como ilícito penal (conforme o artigo 1.º do Código Penal).

Assim, a atividade probatória é essencial para o Estado no exercício da ação penal, que tem de demonstrar em juízo os factos pelos quais pretende condenar uma determinada pessoa a uma concreta sanção jurídico-penal pela realização de determinada conduta, tipificada como crime por aquele. Por outro lado, a prova pode ser encarada como um direito de defesa dos indivíduos, que podem carrear para o processo os factos e elementos que provem a sua versão dos mesmos. Na investigação penal é o Estado, pela ação do Ministério Público – a quem incumbe a direção do inquérito e a recolha de provas (artigos 53.º e 262.º CPP), o responsável por provar os factos pelos quais acusa os indivíduos, não tendo estes de contribuir para a investigação, seja para a sua ilibação ou condenação[149].

No âmbito dos meios probatórios rege o princípio da legalidade, plasmado no artigo 125.º CPP: "são admissíveis as provas que não forem proibidas por lei". Apesar de parecer uma formulação simples, aparentando, numa leitura descomprometida, que o legislador admite todas as provas desde que não sejam proibidas pela lei, este princípio "encontra e enfrenta no seu itinerário tópicos problemáticos como os da liberdade de aquisição probatória, da admissibilidade de provas atípicas, da fungibilidade das formas probatórias e da (não) taxatividade dos métodos proibidos"[150].

c) Defender a democracia política, assegurar e incentivar a participação democrática dos cidadãos na resolução dos problemas nacionais;
d) Promover o bem-estar e a qualidade de vida do povo e a igualdade real entre os portugueses, bem como a efetivação dos direitos económicos, sociais, culturais e ambientais, mediante a transformação e modernização das estruturas económicas e sociais;
e) Proteger e valorizar o património cultural do povo português, defender a natureza e o ambiente, preservar os recursos naturais e assegurar um correto ordenamento do território;
f) Assegurar o ensino e a valorização permanente, defender o uso e promover a difusão internacional da língua portuguesa;
g) Promover o desenvolvimento harmonioso de todo o território nacional, tendo em conta, designadamente, o carácter ultraperiférico dos arquipélagos dos Açores e da Madeira;
h) Promover a igualdade entre homens e mulheres" (negrito nosso).

[149] Podendo o arguido remeter-se ao silêncio (artigo 61.º n.º 1 d) e 345.º CPP), e mesmo que não o faça, não recai sobre ele o dever de falar verdade (apenas tendo de responder com verdade às perguntas feitas pela sua identidade, filiação, freguesia e concelho de naturalidade, data de nascimento, estado civil, profissão, residência, local de trabalho – artigo 141.º n.º 3 e 342 CPP).

[150] Silva, Sandra Oliveira e. "Legalidade da prova e provas proibidas." *Revista Portuguesa de Ciência Criminal*, 2011, ano 21, número 4: 545-591. Página 546.

Em primeiro lugar, é necessário referir que a atividade probatória se encontra necessariamente delimitada por um tema – o *thema probandum* – plasmado no artigo 124.º CPP, sendo a ideia "reitora em matéria de admissibilidade da prova é da mais ampla utilização de todas as técnicas e fontes de conhecimento que se revelem idóneas e úteis" [151] à sua verificação. Assim, para a prova em juízo dos factos, o julgador pode utilizar, indiferentemente, os meios tipificados para o efeito, sendo discutido, na doutrina e jurisprudência, a possibilidade de utilização de provas atípicas[152], com a limitação das provas que forem consideradas proibidas ou a sua valoração vedada.

No artigo 126.º CPP encontra-se o reforço do princípio da legalidade e limite à descoberta da verdade material, estabelecendo-se os meios e métodos proibidos de prova[153]. As proibições de prova constituem os limites à atividade investigatória e probatória – fazendo

[151] Silva, Sandra Oliveira e. "Legalidade da prova e provas proibidas." *Revista Portuguesa de Ciência Criminal*, 2011, ano 21, número 4: 545-591. Página 552. Entende a Autora que a "uma qualquer diligência de prova apenas deverá ser recusada quando não se revele útil à descoberta da verdade (*frustra probatur quod probatum non revelat*), seja por não estar referida ao objeto da prova (utilidade abstrata), seja por se mostrar redundante, supérflua ou desnecessária à decisão (utilidade concreta)" – página 552.

[152] Para mais desenvolvimentos sobre o tema consultar entre outros: Silva, Sandra Oliveira e. "Legalidade da prova e provas proibidas." *Revista Portuguesa de Ciência Criminal*, 2011, ano 21, número 4: 545-591. Página 561 e seguintes; Andrade, Manuel da Costa. "Sobre a valoração, como meio de prova em processo penal, das gravações produzidas por particulares" *Estudos em Homenagem ao Professor Doutor Eduardo Correia*, 1994, número especial do Boletim da Faculdade de Direito da Universidade de Coimbra, vol. I, Coimbra: 545-622; Andrade, Manuel da Costa. *Sobre as proibições de prova em processo penal*, Coimbra: Coimbra Editora, 2006 (reimpressão); Correia, João Conde. "A distinção entre a prova proibida por violação de direitos fundamentais e a prova nula, numa perspectiva essencialmente jurisprudencial". *Revista do CEJ*, n.º 4 (n.º especial), 1.º semestre, 2006: 175-202. Mendes, Paulo de Sousa. "As proibições de prova no processo penal". *Jornadas de Direito Processual Penal e Direitos Fundamentais*, coordenação científica: Maria Fernanda Palma, Coimbra: Almedina, 2004: 133-154; Seiça, Alberto Medina de. "Legalidade da prova e Reconhecimentos «atípicos» em processo penal: notas à margem de jurisprudência (quase) constante", *Liber Discipulorum para Jorge de Figueiredo Dias*, organizado por Manuel da Costa Andrade, Coimbra: Coimbra Editora, 2003: 1387 – 1421.

[153] O artigo 126.º CPP dispõe que: "1 - São **nulas, não podendo ser utilizadas**, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas.
2 - São ofensivas da integridade física ou moral das pessoas as provas obtidas, **mesmo que com consentimento** delas, mediante:
a) Perturbação da liberdade de vontade ou de decisão através de maus tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos;
b) Perturbação, por qualquer meio, da capacidade de memória ou de avaliação;
c) Utilização da força, fora dos casos e dos limites permitidos pela lei;
d) Ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto;
e) Promessa de vantagem legalmente inadmissível.
3 - Ressalvados os casos previstos na lei, são **igualmente nulas, não podendo ser utilizadas**, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular.
4 - Se o uso dos métodos de obtenção de provas previstos neste artigo constituir crime, podem aquelas ser utilizadas com o fim exclusivo de proceder contra os agentes do mesmo." (negrito nosso)

apelo aos ensinamentos de Roxin, existem quatro níveis de proibições de produção de prova, sendo que: "a) determinados factos não podem ser objeto da prática da prova (*proibições de temas probatórios*) ou b) determinados meios de prova não podem ser empregues (*proibições de meios probatórios*) ou c) na produção da prova não se pode fazer uso de certos métodos (*proibições de métodos probatórios*) ou se pode d) ordenar ou realizar a obtenção da prova somente por determinadas pessoas (*proibições probatórias relativas*)"[154].

2. Meios de prova e meios de obtenção de prova

Quanto aos meios de prova, encontram-se regulados no Capítulo I do Título II do Livro II, nos artigos 128.º a 169.º CPP, compreendendo a prova testemunhal, as declarações do arguido, do assistente e das partes civis, a prova por acareação e por reconhecimento, a reconstituição do facto, prova pericial e documental.

Os meios de obtenção de prova encontram-se sistematizados nos artigos 171.º a 190.º CPP, compreendendo os exames, revistas e buscas, apreensões e escutas telefónicas. Existem meio de obtenção de prova consagrados em legislação avulsa, de que são exemplo o registo de som e imagem por qualquer meio, consagrado na Lei 5/2002 de 11 de janeiro, respeitante às medidas de combate à criminalidade organizada e económico-financeira; as ações encobertas previstas na Lei 101/2001 de 25 de agosto, respeitante ao regime jurídico das ações encobertas para fins de prevenção e investigação criminal; e ainda os existentes na Lei 109/2009, Lei do Cibercrime. Quanto aos últimos, encontram-se previstos nos seus artigos 12.º a 19.º: preservação expedita de dados, revelação expedita de dados de tráfego, injunção para apresentação ou concessão do acesso a dados, pesquisa e apreensão de dados informáticos, apreensão de correio eletrónico e registos de comunicações de natureza semelhante e interceção de comunicações.

[154] Roxin, Claus, *Derecho Procesal Penal (..)*, página 191, *apud* Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 69.

Na presente investigação ocupar-nos-emos com os meios de obtenção de prova que se dirigem à interceção[155]/ingerência no *conteúdo* das comunicações eletrónicas fechadas, seja por via escrita como falada, possibilitadas através da Internet, meios que se encontram dispersos em diversos normativos e integrados no âmbito dos meios ocultos de investigação – cuja referência e reflexão são incontornáveis.

3. Os meios ocultos de investigação

Tal como o nome indica, os métodos ocultos de investigação são aqueles utilizados na investigação criminal sem que os investigados deles tenham conhecimento, sendo esse o fator que mais lhes confere eficácia. Ou seja, os visados prosseguem a sua vida e atividade sem saber que estão a ser "escutados", "vigiados" ou que convivem com "agentes infiltrados", podendo confidenciar (e na maioria esmagadora das vezes, confidenciando) informações que poderão ser utilizados contra si num processo de investigação criminal.

Conforme Costa Andrade, "numa perspetiva historiográfica os meios ocultos de investigação não representam, em rigor, um *novum*"[156] – que desde os tempos da Inquisição assombram a memória coletiva. O que é novo na experiência atual dos meios de investigação criminal é o "caráter institucionalizado das medidas, a sua legitimação material e formal-procedimental pela ordem jurídica"[157] – de que são exemplo as escutas telefónicas, aplicáveis também às conversações transmitidas por qualquer meio diverso do telefone, ao correio eletrónico e outras formas de transmissão de dados por via telemática, ainda que se encontrem armazenadas em suporte digital, bem como o acesso aos dados gerados pelas mesmas; a

[155] Benjamim da Silva Rodrigues considera que a utilização do termo "interceção em matéria de escutas telefónicas" não foi a mais feliz (com o que concordamos), "visto que a mesma traduz a ideia de que algo é detido (no seu curso normal). O que não poderia acontecer, uma vez que se incorreria numa "restrição ilegítima de um direito fundamental" ao impedir que o investigado pudesse comunicar – como se retira e infere de Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 86 e seguintes.

[156] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 531.

[157] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 532.

localização celular; a interceção de comunicações entre presentes e as ações encobertas para determinados tipos de criminalidade, com a utilização de agentes infiltrados. A generalização e massificação da utilização de métodos ocultos de investigação é também algo novo no quadro da investigação criminal, o que ilustra a "experiência das escutas telefónicas que, hoje, poucas décadas decorridas sobre o início da prática, se contam, em todo o lado por muitos milhares" [158], pondo na mira da investigação a vida privada de um universo à partida indeterminável de pessoas[159].

Apesar das vantagens da eficácia da utilização dos métodos ocultos de investigação, mormente nos crimes considerados como mais graves pela sociedade, sempre existe o reverso da moeda: "a danosidade social, expressa no sacrifício de bens jurídicos e direitos fundamentais"[160]. Os direitos fundamentais dos indivíduos são direta e gravemente atingidos, principalmente pela dimensão de gravação e armazenamento que existe após a "escuta" ou monitorização propriamente dita: "a privacidade/intimidade, mesmo ao nível da *área nuclear inviolável* (…); o direito à palavra e à imagem; a inviolabilidade do domicílio, das telecomunicações e do sigilo profissional, a autodeterminação informacional, etc", sem esquecer que atualmente até os dados relativos às comunicações são facilmente identificáveis e os indivíduos localizáveis, como são exemplo os dados base, de tráfego e de localização. Mas não se pode esquecer que também a nível adjetivo, processual, existem direitos dos indivíduos que são postos em causa: o direito à não autoincriminação – *nemo tenetur ipsum*

---

[158] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 532. No mesmo sentido, e contra a "prática instalada em Portugal de utilização abusiva de escutas telefónicas", consultar: Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal*. 1ª. Coimbra Editora, 2011. Página 55.

[159] Assim é pois apesar de as interceções e gravações das conversações monitorizadas apenas poderem ser autorizadas contra "suspeito ou arguido", "pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido" ou "vítima de crime, mediante o respetivo consentimento, efetivo ou presumido" (conforme o artigo 187.º n.º 4 CPP), é óbvio que quando a escuta está a ser realizada se podem intercetar comunicações entre estas pessoas, contra quem as escutas podem ser autorizadas, e um universo indeterminável de pessoas que com aquelas comunicam, vendo a sua privacidade coartada com a realização da escuta – e que, tal como escreve Fátima Mata-Mouros, "a experiência revela mesmo que na esmagadora maioria dos casos são elas que dominam – as conversas mantidas pelos suspeitos, arguidos ou vítimas com outras pessoas que não são nem suspeitos, nem arguidos, nem vítimas". Como se retira de Mata-Mouros, Fátima. "Escutas telefónicas - o que não muda com a reforma." *Revista do CEJ*, 1º semestre de 2008, número 9: 219-242. Página 238.

[160] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 536.

accusare, "a liberdade de expressão do arguido e o seu estatuto de sujeito processual, o direito a recusar depoimento e, com ele, as relações de confiança intersubjetiva em que a pessoa se realiza"[161].

Face às novas formas de criminalidade, de comunicação e também das tecnologias ao dispor da investigação, o processo penal tem de se adaptar – pois é a realidade que enforma o Direito, e não o contrário[162]. Assim, "hoje, não se levantam muitos mais desafios ao processo penal que assumam a dimensão dos métodos ocultos de investigação"[163]: tendo vindo os direitos de privacidade e intimidade vindo a ceder em prol de investigações tecnicamente sofisticadas, secretas e altamente violadoras daqueles direitos pela sua eficácia e alcance, em prol do combate às formas de criminalidade mais violentas e organizadas e à garantia da segurança, de que o terrorismo é um exemplo flagrante. Como constata Paulo Dá Mesquita, "no plano processual penal o desenvolvimento tecnológico implicou duas linhas problemáticas novas em relação a velhos modelos probatórios: a) a intromissão e o registo, podendo a atividade repressiva penal dos órgãos estaduais envolver as duas cumulativamente ou apenas uma desligada da outra"[164]. A este ponto voltaremos.

Sob o ponto de vista histórico e tendo em conta a evolução legislativa portuguesa, de entre os métodos ocultos de investigação, as escutas telefónicas podem ser apontadas como a sua "primeira forma" e o regime chapéu dos métodos ocultos de investigação – "tanto pelo seu acentuado relevo prático como pelo caráter mais elaborado e aperfeiçoado do seu regime jurídico, modelado ao longo de décadas de produção legislativa, reflexão doutrinal e labor

---

[161] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 536.

[162] Já em 2009 Flávia Noversa Loureiro constatava que "de facto, a criminalidade altamente organizada, como costuma apelidar-se, seja ou não relacionada com crimes de terrorismo, mas quase sempre conectada com associações e redes criminosas, embora a elas não possa reconduzir-se sem mais, coloca problemas muito graves às autoridades judiciárias de cada país, uma vez que para lhes fazer frente, não bastam os meios habitualmente utilizados, sendo precisas não só formas muito mais sofisticadas ao nível tecnológico como muito mais invasivas e potencialmente suscetíveis de afetar esferas privadas de indivíduos, do ponto de vista fáctico" - Loureiro, Flávia Noversa. "A (i)mutabilidade do paradigma processual penal respeitante aos direitos fundamentais em pleno século XXI." Em *Que futuro para o Direito Processual Penal?*, de Mário F. Monte, 269-289. Coimbra Editora, 2009. Página 276.

[163] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 95.

[164] Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 84.

jurisprudencial"[165]. Como exemplo e marco da importância do regime das escutas telefónicas no quadro dos métodos ocultos de investigação no quadro processual português é o artigo 189.º CPP: estende a aplicação do regime das 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, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes".

É importante referir que a reforma operada em 2007 "manteve inalterada a sistematização original de 1987 do capítulo *escutas telefónicas* como quadro global da regulação da interceção e registo das telecomunicações, apesar das alterações tecnológicas e da existência de um lastro de pontuais alterações reveladoras dos limites, e problemas, compressivos dessa categoria como sede abrangente da interceção de dados de comunicações transmitidas através de meios técnicos"[166] – quadro que melhor analisaremos adiante.

Assim, "as escutas telefónicas gozam hoje, no panorama de uma "teoria geral" dos meios ocultos de investigação, de um estatuto de paradigma e arquétipo e figuram como referente obrigatório para o intérprete e aplicador, confrontado com os problemas jurídicos suscitados pelos outros meios ocultos. E que hoje integram um denso e alargado espetro, muito para além das escutas telefónicas"[167]. Partilhamos este entendimento, uma vez que basta a leitura do artigo 189.º CPP para ser evidente a importância que é dada pelo legislador ao regime das escutas telefónicas, sendo aplicável (?) a métodos tão díspares como a interceção de conversações entre presentes, interceção de correio eletrónico e de conversações (ou ficheiros que se as contenham?) que se encontrem armazenadas em suporte digital.

Desta forma, a referência ao regime das escutas telefónicas é obrigatória no estudo de qualquer método de obtenção oculto de prova que se considere, principalmente no que

[165] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 533.
[166] Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 89.
[167] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 533.

move esta investigação – a ingerência no conteúdo das comunicações eletrónicas: até para perceber se é, ou deve ser, o seu regime o "regime-chapéu" dos novos meios ocultos de obtenção de prova que se dirijam às comunicações eletrónicas.

Conforme ensina o Mestre Costa Andrade, o jurista, no âmbito dos métodos ocultos de investigação, deve trilhar o seu caminho balizado por dois enunciados: "Em primeiro lugar, a investigação clandestina veio para ficar, configurando um dado da experiência jurídica atual e, não será arriscado acreditá-lo, do futuro. Em segundo lugar, ela só pode ser pensada, institucionalizada e aplicada aos casos da vida na medida em que for concretamente compatível com o *Rechtskultur* [cultura jurídica] do processo penal do Estado de Direito e não puser em causa aquilo que, naquele processo, persiste como *indisponível* (*Unverfügbares*). Esta última uma consideração que, só por si, vale como um programa político-criminal que aposta na redução drástica do espaço concedido às medidas. A começar pela sua vinculação ao universo contado das formas mais graves de criminalidade"[168], sendo essencial que a doutrina e jurisprudência se debrucem sobre esta questão, contribuindo para a consagração de uma teoria geral dos métodos ocultos de investigação, de modo a reduzir as "comprometedoras inconsistências e assistemicidades e desproporcionadas assimetrias"[169] que hoje se verificam, inclusivamente quando a lei estende a aplicação de um método de obtenção de prova tão exigente nos seus requisitos e pensado para as violações mais graves dos direitos dos cidadãos a métodos completamente distintos na sua *ratio* e nível de violação de direitos fundamentais. Mais ainda quando consagra técnicas de obtenção de prova ainda mais gravosas ao nível da violação daqueles, aos quais se aplica o regime das escutas, exponenciando o efeito violador de direitos fundamentais – como é o caso da gravação de conversações entre presentes.

Já em 2007 Costa Andrade constatava que "só agora a comunidade jurídica começa a despertar para o verdadeiro alcance e para o âmbito dos meios de intromissão oculta nas comunicações eletrónicas, enquanto correlativos das novas formas de comunicar permitidas

[168] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 539.
[169] Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009. Página 538.

pelas inovações tecnológicas – dos quais se destaca todo o mundo informático e a rede universal da Internet"[170]. Como escreve Rita Castanheira Neves, "o essencial é não mais permitir que toda uma nova realidade de possibilidades de obtenção de prova se reconduza aos métodos tradicionais, sem preocupações com o princípio da legalidade e forçando uma convivência de regulamentações que não assentam verdadeiramente sobre os mesmos elementos empíricos"[171]. A questão impõe-se: passados 10 anos sobre a reforma de 2007 terá o legislador despertado para a importância das comunicações eletrónicas e resolvido as disparidades em volta do seu regime de obtenção como prova?

4. As Escutas Telefónicas

a) Considerações introdutórias

Com base na possibilidade aberta com a exceção à inviolabilidade das comunicações no âmbito da investigação criminal plasmada no artigo 34.º n.º 4 CRP, o Código de Processo Penal consagra como meios de obtenção de prova contendentes com a intromissão nas comunicações dos indivíduos a apreensão de correspondência e as escutas telefónicas.

É importante realçar, de novo, que qualquer restrição aos direitos fundamentais em causa tem que ser "norteada por estritas exigências de proporcionalidade e adequação, respeitando-se solenemente os princípios de reserva de juiz e de lei", uma vez que "só é legalmente possível perseguir a verdade material através de meios de prova restritivos de certos direitos, liberdades e garantia (…) se esses mesmos meios de obtenção de prova estiverem legalmente previstos e regulados com razoável clareza e determinabilidade, no respeito pelo princípio da legalidade"[172].

---

[170] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 97.

[171] Neves, Rita Castanheira. As ingerências nas comunicações electónicas em Processo Penal. 1ª. Coimbra Editora, 2011. Página 102.

[172] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 55. No mesmo sentido entende Flávia Noversa Loureiro: "Não podemos pretender que se *arranquem olhos* dentro do modelo processual português que queremos operativo, mas justo, por isso, teremos que diariamente propugnar pelo equilíbrio possível entre as duas ordens de grandeza que estão em jogo" – " por um lado, a eficácia no combate ao crime para defesa da comunidade, por outro, a proteção dos direitos fundamentais dos indivíduos em geral e dos arguidos em particular" – como se retira de Loureiro, Flávia

O artigo 189.º CPP, no seu número 1, consagra que "O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às **conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone**, designadamente **correio eletrónico ou outras formas de transmissão de dados por via telemática**, mesmo que se encontrem **guardadas em suporte digital**, e à **interceção das comunicações entre presentes**".

Em virtude desta extensão operada pelo legislador à aplicação do regime das escutas telefónicas à interceção de outros (e tão variados) tipos de comunicações, *ex vi* artigo 189.º n.º 1 CPP, consideramos, no seguimento do pensamento de Costa Andrade, como atrás explanado, que é obrigatório o excurso sobre o regime das escutas telefónicas, que são a "primeira forma" dos métodos ocultos de investigação, e que, ainda hoje, pela mão do artigo 189.º n.º 1 CPP, influenciam o regime aplicado a outras realidades, que não as conversações telefónicas. Assim entendemos pois poderá possibilitar a compreensão do regime que se discute ser de aplicar, ou não, à interceção ou monitorização do conteúdo das comunicações eletrónicas.

Tal como Benjamim da Silva Rodrigues, consideramos que a expressão "escutas telefónicas" operada pelo Código de Processo Penal não a mais feliz, nem a mais adequada – "visto que a ingerência nas comunicações telefónicas abrange diversas fases materiais, de entre as quais, a «escuta» é apenas uma delas, havendo, ainda, que referir que o ato da «gravação» é o que concede, a esta forma de intervenção nas comunicações pessoais, em tempo real, uma especificidade que se repercute ao nível da sua elevada danosidade social"[173], o que leva à compressão dos direitos fundamentais dos indivíduos, consagrados pela Constituição. Para além disto, pela ação do artigo 189.º CPP o regime das "escutas" é aplicável a um universo de conversações e ficheiros que podem não ser "escutáveis" – seja porque a monitorização é dirigida ao correio eletrónico ou a outros meios de conversação por escrito, seja porque se dirige a ficheiros informáticos armazenados que contêm (*ou* podem conter) aquelas conversações escritas ou faladas. Assim, quando aplicado à ingerência da investigação criminal nas comunicações eletrónicas, a fase da "escuta" pode nem sequer

Noversa. "A (i)mutabilidade do paradigma processual penal respeitante aos direitos fundamentais em pleno século XXI." Em *Que futuro para o Direito Processual Penal?*, de Mário F. Monte, 269-289. Coimbra Editora, 2009. Página 289.

[173] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 70.

existir – quando se trata da interceção de comunicações eletrónicas escritas, só ocorrendo quando se tratem de comunicações de voz, através do sistema *Voice OverIP*, ou quando se proceda à interceção (apreensão?) de ficheiros áudio, armazenados em suporte digital.

É inegável que as escutas telefónicas são um meio bastante eficaz para trazer para a investigação criminal informações que, por outro meio, seriam muito difíceis ou mesmo impossíveis de obter (que, aliás, são o fundamento para a sua utilização). No entanto, e como relembra Francisco Marcolino de Jesus, "se usadas sem moderação, esquecendo que são *ultima ratio*, se não forem objeto de permanente controlo judicial, estaremos a contribuir, seguramente, para a transformação do Estado-de-direito em Estado-policial"[174]. Ou seja, na aplicação deste meio particular de obtenção de prova, exige-se ao Estado uma ponderação *ex ante*, em abstrato, no momento em que consagra e regula o meio de obtenção de prova, mas também uma ponderação em concreto, quanto à situação a ser investigada e em que se pretende lançar mão deste meio de obtenção de prova – necessidade de operar a "concordância prática"[175] entre os pontos de tensão identificados: "eficácia no combate ao crime para defesa da comunidade" e a "proteção dos direitos fundamentais dos indivíduos em geral e dos arguidos em particular"[176]. Se assim não for, inverte-se a função do Estado em nome de interesses securitários, perseguindo a prática criminosa mesmo antes de ela existir, "não faltando quem reivindique que a investigação se antecipe para evitar a prática do crime, dando-se um fenómeno de intervenção pró-ativa em substituição de uma resposta reativa por parte das autoridades formais de controlo"[177].

---

[174] Jesus, Francisco Marcolino de. *Os meios de obtenção de prova em Processo Penal.* 2ª - Reimpressão. Almedina, 2015. Página 284.

[175] Dias, Figueiredo. "Direito Processual Penal - Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por Maria João Antunes, Assistente da Faculdade de Direito da Universidade de Coimbra." Coimbra: Secção de Textos da Faculdade de Direito da Universidade de Coimbra, 1998/1999. Página 24 e seguintes.

[176] Loureiro, Flávia Noversa. "A (i)mutabilidade do paradigma processual penal respeitante aos direitos fundamentais em pleno século XXI." Em *Que futuro para o Direito Processual Penal?*, de Mário F. Monte, 269-289. Coimbra Editora, 2009. Página 275.

[177] Como se retira de Rodrigues, Cláudio Lima. "Dos pressupostos materiais de autorização de uma escuta telefónica." *verbojuridico.net.* Editado por Verbo Jurídico. Fevereiro de 2013. http://www.verbojuridico.net/ficheiros/doutrina/ppenal/claudiolimarodrigues_autorizacaoescutatelefonica.pdf (acedido em 27 de Dezembro de 2016). Página 10.
Há também quem questione se não fará sentido "a admissibilidade das escutas telefónicas fora do domínio da investigação criminal, «noutro tempo e noutro espaço que não o delimitado pelo processo penal», nomeadamente no âmbito dos serviços de inteligência e das suas atividades de segurança interna dos Estados" – questão enunciada em Lopes, José Mouraz. "Escutas telefónicas: seis teses e uma conclusão." *Revista do Ministério Público*, Outubro-Dezembro de 2005, ano 26: 139-151. Página 143. No mesmo sentido entendia já

Como constata Flávia Noversa Loureiro, as mentalidades e exigências das sociedades têm vindo a ser alteradas com o passar do tempo, e se numa primeira fase o "direito fundamental do homem, enquanto cidadão, era (…) ter por garantido um espaço em que o Estado, a comunidade enquanto ser coletivo, não poderia penetrar, sob qualquer motivação ou justificação"[178], rapidamente se compreendeu que o afastamento do Estado não iria assegurar que as suas liberdades pessoais não fossem afetadas, sendo este "chamado a zonas donde tinha sido expulso a todo o custo" perante a afirmação da *sociedade de risco*, vendo-se "paradoxalmente, conformado a duas linhas excêntricas: por um lado, a sua atuação é exigida, e com graus celeridade e eficiência até aí não pensáveis sequer, em campos para os quais, na grande maioria das vezes, não é preparado para agir, nem é fácil fazê-lo sem interferir na esfera de liberdade de cada um; por outro, é chamado a consegui-lo, ainda assim, com respeito por um núcleo intangível de direitos e liberdades que não pode suportar-se ver afetado, sob pena de se descaracterizar o próprio Estado de Direito"[179]. Assim é pois a sociedade exige ao Estado respostas eficazes quanto a fenómenos graves, de que é exemplo o tráfico de estupefacientes, de pessoas e o terrorismo, ao mesmo tempo que repugna a intromissão daquele na esfera dos seus direitos fundamentais, nomeadamente a intimidade da sua vida privada, confidencialidade, reserva de dados, etc.

Em jeito de conclusão introdutória, poderemos afirmar, com Cristina Ribeiro, que "as normas processuais penais que hoje consagram as escutas telefónicas como um meio de obtenção de prova procuram fazer a ponderação entre os interesses e direitos conflituantes e espelham a tensão dialética existente entre: a) por um lado, garantir a tutela dos direitos, liberdades e garantias dos cidadãos, b) por outro, salvaguardar os interesses mais relevantes

---

Teles Pereira, em 2002: "tem de ser encarada seriamente a questão da possibilidade de realização de interceções nas comunicações, a realizar segundo um modelo restritivo, "amigo" dos direitos fundamentais (v.g. autorização, caso a caso, por uma comissão de magistrados" – e se esta opção não for considerada como viável, no âmbito de um Estado de Direito democrático, entende o Autor que os serviços de informação se arriscam a ser uma "benfeitoria voluptuária que, para mais, criam uma aparência de segurança onde ela verdadeiramente não existe"- como se retira e infere de Pereira, J. A. Teles. "O 11 de Setembro e o debate sobre o modelo de Serviços de Informações em Portugal." *Revista do Ministério Público*, Janeiro/Março de 2002, ano 23: 155-164. Páginas 163 e 164.

[178] Loureiro, Flávia Noversa. "A (i)mutabilidade do paradigma processual penal respeitante aos direitos fundamentais em pleno século XXI." Em *Que futuro para o Direito Processual Penal?*, de Mário F. Monte, 269-289. Coimbra Editora, 2009. Página 271.

[179] Como se retira e infere de Loureiro, Flávia Noversa. "A (i)mutabilidade do paradigma processual penal respeitante aos direitos fundamentais em pleno século XXI." Em *Que futuro para o Direito Processual Penal?*, de Mário F. Monte, 269-289. Coimbra Editora, 2009. Página 271.

da eficácia da investigação criminal e o interesse comunitário no cumprimento das normas penais, garantindo o *ius puniendi* do Estado"[180] – o que em última *ratio* também consiste na tutela dos direitos fundamentais dos cidadãos e interesses da comunidade, "os bens jurídicos em causa em cada tipo legal (a vida, a integridade física, a liberdade sexual, etc.)". Por isso o Estado vive nesta constante tensão – pretendendo que a paz impere e que a prática criminosa seja reprimida (e punida, nos casos em que não o consiga ser), tendo ainda que respeitar os direitos de todos os indivíduos – em que se inserem os suspeitos e arguidos.

b) O regime das escutas telefónicas

O legislador consagrou que "a interceção e a gravação de conversações ou comunicações telefónicas **só podem ser autorizadas durante o inquérito**, 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**, por **despacho fundamentado do juiz de instrução** e **mediante requerimento do Ministério Público**", para o catálogo de crimes que estabelece – artigo 187.º n.º 1 e 2 CPP.

Em primeiro lugar, para que as escutas telefónicas possam, em abstrato, ser aplicáveis, é necessário que exista um inquérito instaurado (artigos 262.º e seguintes CPP) – "e para tanto, é necessária a notícia de um crime [artigo 241.º CPP], ou seja, em princípio, o campo de utilização das escutas telefónicas no nosso país reconduz-se à investigação de crimes já cometidos ou, pelo menos já iniciados"[181], não podendo, entre nós, as escutas ser realizadas preventivamente à notícia de um crime[182]. Apesar de não ser necessária a

[180] Ribeiro, Cristina. "Escutas telefónicas: pontos de discussão e perspetivas de reforma." *Revista do Ministério Público*, Outubro-Dezembro de 2003, ano 24: 67-89. Página 68.

[181] Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014. Página 789 e Jesus, Francisco Marcolino de. *Os meios de obtenção de prova em Processo Penal.* 2ª - Reimpressão. Almedina, 2015. Página 296.

[182] Apesar haver quem entenda que bastantes vezes as escutas possuem mais importância na prevenção de crimes que "se suspeita poderem vir a ser cometidos" do que nos crimes já consumados – como se retira e infere de Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014. Página 789. No mesmo sentido entende Fátima Mata-Mouros, indo mais longe e afirmando que "quem trabalha em investigação sabe perfeitamente que não é essa a vocação das escutas" – de se reconduzir à investigação de crimes já cometidos ou iniciados. Esta Autora afirma que "A sua vocação

consumação do crime, sempre "supõe a realização de um *iter* penalmente relevante, isto é, só pode ser ordenada uma escuta telefónica se tiverem sido cometidos atos de execução ou atos preparatórios puníveis"[183].

Em segundo lugar, as escutas telefónicas apenas podem utilizadas na investigação do catálogo de crimes definido pelo legislador, tendo este optado, na determinação do catálogo de crimes em que é admissível o recurso às escutas, por um critério misto: determinando um catálogo de crimes a que as escutas se podem dirigir expressamente delimitado, e estabelecendo um critério de aplicação relativo à moldura penal: são aplicáveis a "crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos" – artigo 187.º n.º 1 e 2 CPP.

Para que se utilizem as escutas telefónicas no caso concreto é necessário que o juiz de instrução[184] profira despacho fundamentado[185], e apenas nos casos em que haja "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" – o que constitui a afirmação da natureza excecional do regime das escutas, demonstrando que estas devem ser utilizadas como última

[da aplicação do regime das escutas] é a recolha de informação e a sua especial aptidão joga-se na compreensão da estrutura e organizações criminosas, nas chamadas investigações estruturais", o que é "precisamente o inverso das limitações que decorrem da nossa Lei Fundamental e do regime estabelecido no nosso Código de Processo Penal" – conforme se retira de Mata-Mouros, Fátima. "Escutas telefónicas - o que não muda com a reforma." *Revista do CEJ*, 1º semestre de 2008, número 9: 219-242. Página 241. Por isso faria sentido, tal como incentiva a Autora, que fossem disponibilizados ao público os dados relativos à realização de escutas telefónicas, e ainda identificar "de entre as investigações realizadas com recurso a escutas telefónicas, qual a expressão dos casos em que os crimes investigados vêm, afinal, a ser cometidos já depois de iniciada a interceção".

[183] Albuquerque, Paulo Pinto de. *Comentário do Regime Geral das Contra-Ordenações à Luz da Constituição da República e da Convenção Europeia dos Direitos do Homem.* Universidade Católica Editora, 2011. Página 526.

[184] Conforme José Mouraz Lopes, também entendemos que "A necessidade absoluta da intervenção jurisdicional, para que se legitime esta forma de obtenção de prova, surge assim como a última e única forma de validar o que contraria substancialmente quer a estrutura formal de um ideal processo penal, quer, sobretudo, pela difícil justificação, mesmo ancorada no princípio da proporcionalidade, da violação grosseira da privacidade e intimidade de quem está em comunicação" – retirado de Lopes, José Mouraz. "Escutas telefónicas: seis teses e uma conclusão." *Revista do Ministério Público*, Outubro-Dezembro de 2005, ano 26: 139-151. Página 144.

[185] A fundamentação é uma das principais exigências de um regime que se quer democrático, para que todos os sujeitos processuais compreendam os motivos que fundaram tal decisão, e mesmo para ser objeto de reexame em qualquer instância, e um requisito formal para aplicação das escutas telefónicas ao caso concreto – conforme o artigo 205.º da CRP e 187.º n.º 1 CPP.

ratio, nos casos mais difíceis de obtenção de prova, em que sejam o meio mais adequado para a sua recolha, e por isso de forma subsidiária[186].

Para além destes requisitos, o legislador previu no artigo 187.º n.º 4 CPP o universo de pessoas "escutáveis": "A interceção e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra: a) Suspeito ou arguido; b) Pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou c) Vítima de crime, mediante o respetivo consentimento, efetivo ou presumido", estando a interceção e a gravação de conversações ou comunicações entre o arguido e o seu defensor proibidas, "salvo se o juiz tiver fundadas razões para crer que elas constituem objeto ou elemento de crime" (conforme o artigo 187.º n.º 5 CPP).

Quanto ao conceito de arguido, é facilmente identificável: é aquele contra quem corre um inquérito e relação ao qual haja suspeita fundada da prática de crime, tendo prestado declarações perante qualquer autoridade judiciária ou órgão de polícia criminal; a quem tenha de ser aplicada a qualquer pessoa uma medida de coação ou de garantia patrimonial; aquele que for detido nos termos e para os efeitos previstos nos artigos 254.º a 261.º; ou aquele de for levantado auto de notícia que o dê como agente de um crime e aquele lhe for comunicado, salvo se a notícia for manifestamente infundada – conforme o artigo 58.º n.º 1 CPP.

O conceito de "suspeito" é algo mais amplo e indefinido, uma vez que pode não estar identificado no momento em que se autoriza a realização da escuta – "bastando, para tal, que haja indícios de que uma tal pessoa seja suspeita e que esses indícios apontem para um concreto aparelho que permita a posterior identificação do «suspeito»"[187 e 188], cabendo ao

[186] Fátima Mata-Mouros, já após a reforma de 2007, entendia que o princípio de subsidiariedade de aplicação das escutas telefónicas é inexequível: "é que não sendo viável uma graduação em abstrato das medidas de investigação em função de critérios como o da respetiva potencialidade lesiva para os direitos dos visados ou do grau de eficiência que oferecem para a investigação de cada tipo de crime, dificilmente a cláusula de subsidiariedade poderá adquirir eficácia prática". Mata-Mouros, Fátima. "Escutas telefónicas - o que não muda com a reforma." *Revista do CEJ*, 1º semestre de 2008, número 9: 219-242. Página 241.

[187] Leite, Inês Ferreira. "O novo regime das escutas telefónicas. Uma visão panorâmica sobre a reforma de 2007." Em *Direito da Investigação Criminal e da Prova*, de AA. VV. Almedina, 2014. Página 262. No mesmo sentido entende Jesus, Francisco Marcolino de. *Os meios de obtenção de prova em Processo Penal.* 2ª - Reimpressão. Almedina, 2015. Página 291.

[188] Fátima Mata-Mouros considera que a definição do universo de pessoas escutáveis não irá por termo à proliferação da utilização das escutas telefónicas, seja porque o legislador não adiantou, em 2007, a definição de "suspeito" – e "por norma, a polícia só solicita escutas a pessoas consideradas «suspeitas» de práticas

Ministério Público definir quem é que considera como suspeito no requerimento de realização das escutas, "estando vedado ao Juiz de Instrução Criminal contestar esta qualificação, salvo se esta for manifestamente ilegal"[189].

As vítimas podem ser os titulares do bem jurídico lesado com a atividade criminosa e que têm faculdade de se constituir assistentes, ou também os "titulares de um bem jurídico que seja, de modo mediato ou difuso, tutelado pelo tipo, quando se trate de crime de perigo ou que tutele uma multiplicidade de bens"[190]. Quanto a estas, cabe ao Ministério Público, no requerimento para realização das interceções telefónicas, juntar o consentimento da(s) vítima(s), e ainda indicar as razões de facto e de direito que entende justificar a interceção, das quais cabe decisão de mérito ao Juiz de Instrução Criminal – uma vez que é a este que cabe a decisão de constituição de assistente e de reconhecimento da qualidade de lesado (artigo 68.º n.º 4 e 5 - não relevando aqui a competência do juiz de julgamento para tal, uma vez que as escutas nunca poderão ser autorizadas e realizadas nesta fase, artigo 71.º CPP).

Quanto ao conceito de "intermediário", é ainda mais difícil a sua concretização. Inês Ferreira Leite entende que é "um núncio, um mero mensageiro cuja atividade não se revela causal para a prática do crime ou crimes, ou até, que atua sem dolo de comparticipação"[191].

Quanto à fundamentação exigida para o despacho de autorização da realização das escutas, não parece que deva ser exigida uma fundamentação exaustiva, com uma "exigência de precisão que torne inviável a sua concretização" [192]: apenas é possível um "juízo tanto mais genérico quanto mais próximo estamos da fase inicial da investigação sendo certo que, mesmo dentro dos crimes do catálogo, alguns existem que, pela sua gravidade e especificidade imprimem desde logo uma ideia de indispensabilidade da escuta (v.g.

---

criminosas, pelo menos na perspetiva dos investigadores", seja porque o "juiz não tem efetiva possibilidade prática de contrariar a polícia na sugestão que os investigadores lhe apresentam dever considerar-se esta ou aquela pessoa como suspeita" - Mata-Mouros, Fátima. "Escutas telefónicas - o que não muda com a reforma." *Revista do CEJ*, 1º semestre de 2008, número 9: 219-242. Página 238.

[189] Leite, Inês Ferreira. "O novo regime das escutas telefónicas. Uma visão panorâmica sobre a reforma de 2007." Em *Direito da Investigação Criminal e da Prova*, de AA. VV. Almedina, 2014. Página 262.

[190] Leite, Inês Ferreira. "O novo regime das escutas telefónicas. Uma visão panorâmica sobre a reforma de 2007." Em *Direito da Investigação Criminal e da Prova*, de AA. VV. Almedina, 2014. Página 263.

[191] Leite, Inês Ferreira. "O novo regime das escutas telefónicas. Uma visão panorâmica sobre a reforma de 2007." Em *Direito da Investigação Criminal e da Prova*, de AA. VV. Almedina, 2014. Página 263.

[192] Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014. Página 791.

terrorismo; criminalidade organizada)"[193]. Benjamim da Silva Rodrigues relembra que o despacho que autoriza a realização da escuta decide uma questão interlocutória, isto é, "da necessidade de ordenar ou autorizar a medida de interceção e gravação de conversações ou comunicações levadas a cabo por telefone, no âmbito de um processo judicial em curso"[194].

Este Autor considera que a fundamentação exigida pelos artigos 187.º n.º 1 e 190.º CPP considera-se satisfeita se estiverem descritos: "i) indicação de existência de *indícios determinados* de que alguém cometeu um dos crimes do catálogo ou cuja moldura penal é superior a três anos (artigo 187.º n.º 1 CPP); ii) *idoneidade e necessidade da medida* para a descoberta da verdade ou para a prova; iii) *delimitação subjetiva*: a pessoa ser objeto da ingerência; iv) *delimitação objetiva:* telefone(s) objeto(s) da medida (número de telefone a intervir); v) *indício, duração e cessação da medida*; vi) A *razão de ciência* em que se baseia o juízo de admissibilidade da intervenção; vii) cumprimento de alguns *deveres acessórios:* entrega cíclica (de relatórios) para controlo, das gravações efetuadas"[195]. Este Mestre realça ainda que "não se deve cair no exagero de que a motivação seja tão completa como se se tivesse a certeza de que o investigado cometeu o crime, pois, a ser assim, ficaria deslegitimado o recurso a tal meio visto que os factos teriam já a clareza e concisão suficientes para autonomizarem e fundarem um juízo de acusação"[196]. É necessário que o Juiz de Instrução realize um "juízo de prognose face à situação concreta das investigações e aos elementos recolhidos, abrangendo a sua complexidade, mas também a sua eficácia"[197], contendo os factos "que permitam inferir que, naquele caso concreto, apenas as escutas telefónicas têm aptidões probatórias, falhando os demais meios probatórios ou tornando-se a obtenção de prova dificilmente acessível e com elevados custos"[198]. Trata-se do princípio da

[193] Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014. Página 791.
[194] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 226.
[195] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 226.
[196] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 227.
[197] Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014. Página 789.
[198] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 266.

necessidade da medida, exprimindo a opção pelo menor sacrifício dos direitos fundamentais dos indivíduos em razão da investigação criminal, apenas se podendo recorrer a um meio de obtenção de prova tão atentatório daqueles, como são as escutas telefónicas (e principalmente na sua dimensão de gravação) nos casos em que aquelas sejam idóneas: "no sentido de prognóstico (positivo) favorável da medida de intervenção, visto que ela produz dados relevantes (e imprescindíveis) para os resultados da investigação aberta e incipiente"[199]. Tem de haver, por isso, consciência do que se pretende alcançar com a investigação – ou então, realizar um juízo de valor que permita inferir quais os resultados que determinados meios de prova que permitirão alcançar esses conhecimentos – para determinar se as escutas telefónicas são, no caso concreto o único meio idóneo para alcançar as informações que se necessita carrear para a investigação[200].

Quanto a este aspeto, Inês Ferreira Leite considera que é necessário que "se faça dois juízos: a) existem já algumas provas que sustentam alguns indícios, mas as mesmas são contraditórias face à responsabilidade penal dos agentes ou ao modo como participaram do crime, havendo uma contradição insanável que impede a dedução da acusação, salvo se forem realizadas as escutas (essencialidade face à descoberta da verdade); ou b) o Ministério Público está a par do *modus operandi* dos agentes e tem conhecimentos fácticos sobre a prática do crime, contudo, precisamente por causa do específico modo de agir daqueles, não será possível fazer prova de tais factos em julgamento (impossibilidade ou dificuldade de obtenção da prova)"[201].

No entanto, como bem relembra Carlos Adérito Teixeira, com o requisito e matriz das escutas telefónicas como última *ratio* não significa que elas têm de ser "o último meio a lançar-se mão, num sentido cronológico, mas sim o «*último» no plano lógico* ou lógico-funcional" [202] – pois, se assim não fosse, só no final do inquérito e após a utilização de todos

[199] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 267.
[200] Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014. Página 790.
[201] Leite, Inês Ferreira. "O novo regime das escutas telefónicas. Uma visão panorâmica sobre a reforma de 2007." Em *Direito da Investigação Criminal e da Prova*, de AA. VV. Almedina, 2014. Página 258.
[202] Teixeira, Carlos Adérito. "Escutas telefónicas: a mudança de paradigma e os velhos e os novos problemas." *Revista do CEJ*, 1º semestre de 2008, nº 9: 243-295. Página 245.

os meios de obtenção de prova que se consideram, e são, menos gravosos sob o ponto de vista dos direitos fundamentais dos investigados, é que se poderia recorrer à utilização das escutas – o que "nessa altura, já não se justificaria porque a prova estaria coligida ou já não se poderia obter porque a oportunidade efetiva ter-se-ia ignorado"[203 e 204].

Quanto ao grau de suspeita que é exigido para a autorização das escutas telefónicas, Francisco Marcolino de Jesus considera que o legislador deveria ter densificado o grau de suspeita que exige da identidade do agente e da prática do crime para que seja admissível a utilização das escutas telefónicas no caso concreto. Assim, considera que no que respeita ao requisito material de autorização das escutas deveria "ter feito «a exigência de uma suspeita, substanciada em factos e qualificada no grau de plausibilidade»"[205] – uma vez que, "ao não o fazer permitiu que as escutas continuem, apesar de excecionais, a poderem ser realizadas com inusitada frequência porque o conceito de suspeito é demasiado amplo"[206].

---

[203] Teixeira, Carlos Adérito. "Escutas telefónicas: a mudança de paradigma e os velhos e os novos problemas." *Revista do CEJ*, 1º semestre de 2008, nº 9: 243-295. Página 245.

[204] No mesmo sentido entendem Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014. Página 792: "Continua a ser possível recorrer às escutas telefónicas logo como primeiro meio de obtenção de prova utilizado quando o juiz de instrução se convença, em face dos concretos dados factuais trazidos pelo MP, que elas são a única diligência capaz de importar para os autos elementos probatórios aptos à descoberta da verdade. Se, ao invés, o Ministério Público tiver ao seu dispor qualquer outro meio que assegure o mesmo resultado, é esse que deverá ser utilizado, sendo inadmissível qualquer argumentação em contrário, maxime baseada em maior dispêndio de tempo ou recursos materiais e/ou humanos". E ainda André Lamas Leite, em Leite, André Lamas. "Entre Péricles e Sísifo: o novo regime legal das escutas telefónicas." *Revista Portuguesa de Ciência Criminal*, Outubro-Dezembro de 2007, ano 17: 613-679. Página 626: Mantendo o entendimento que possuía antes de 2007, considera que "continua a ser possível lançar-se mão das esctuas *logo como primeiro meio de obtenção de prova utilizado*, quand - *e apenas nesta hipótese* - o juiz de instrução se convença, em face dos concretos dados factuais trazidos pelo MP, que ela é a *única diligência capaz de fazer carrear para os autos elementos probatórios aptos à descoberta da verdade*".

[205] Jesus, Francisco Marcolino de. *Os meios de obtenção de prova em Processo Penal.* 2ª - Reimpressão. Almedina, 2015. Página 291 – de resto, como entende costa andrade – bruscamente no verão passado.

[206] Jesus, Francisco Marcolino de. *Os meios de obtenção de prova em Processo Penal.* 2ª - Reimpressão. Almedina, 2015. Página 291. No mesmo sentido entende Fátima Mata-Mouros: esta Autora considera que a definição do universo de pessoas escutáveis não irá por termo à proliferação da utilização das escutas telefónicas, seja porque o legislador não adiantou, em 2007, a definição de "suspeito" – e "por norma, a polícia só solicita escutas a pessoas consideradas «suspeitas» de práticas criminosas, pelo menos na perspetiva dos investigadores", seja porque o "juiz não tem efetiva possibilidade prática de contrariar a polícia na sugestão que os investigadores lhe apresentam dever considerar-se esta ou aquela pessoa como suspeita" - Mata-Mouros, Fátima. "Escutas telefónicas - o que não muda com a reforma." *Revista do CEJ*, 1º semestre de 2008, número 9: 219-242. Página 238.

5. A Lei do Cibercrime

A Lei do Cibercrime, Lei 109/2009, entrou em vigor em Portugal no dia 15 de outubro de 2009. Trata-se de uma lei especial avulsa que contém tipos legais de crime relacionados com a informática e a sua utilização, bem como meios de obtenção de prova dirigidos à recolha de prova no âmbito da utilização de sistemas informáticos, a denominada prova em suporte eletrónico.

No que à presente investigação diz respeito, a ingerência nas comunicações eletrónicas e o acesso ao seu conteúdo, esta Lei é de fundamental importância, pois se trata da Lei que consagra os meios de obtenção de prova de "apreensão de correio eletrónico" e "interceção de comunicações eletrónicas"– os meios de obtenção de prova a considerar, para o catálogo de crimes nesses normativos previstos, no que toca à ingerência no conteúdo[207] das comunicações eletrónicas (para além do malogrado artigo 189.º n.º 1 CPP).

A consagração destes meios de obtenção de prova fora do Código de Processo Penal, em relação a distintos catálogos de crimes, e sua "convivência" com o artigo 189.º CPP levanta a questão de saber qual é, afinal, o reduto de aplicabilidade do artigo 189.º n.º 1 CPP e dos artigos 17.º e 18.º da Lei do Cibercrime, e qual a destrinça que deve ser feita entre estes meios de obtenção de prova pelo intérprete e aplicador no que toca às comunicações eletrónicas.

a) O caminho até à sua consagração – de 1991 a 2004

Até à entrada em vigor da Lei do Cibercrime, em 2009, vigorou a Lei da Criminalidade Informática – a Lei 109/91, de 17 de agosto.

[207] Quanto aos dados informáticos gerados pelas telecomunicações e o interesse do seu acesso, consultar a recentíssima Lei Orgânica 4/2017, disponível em https://dre.pt/application/conteudo/108052020, acedida e consultada a 01/09/2017, que consagra o "procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa", e que se prende com o acesso aos "dados de base", "dados de localização de equipamento" e "dados de tráfego" relativamente aos "dados de telecomunicações" e "dados de Internet".

No entanto, esta Lei não possuía disposições processuais relativas à criminalidade informática; apenas se propunha a regular a matéria substantiva da mesma, prevendo tipos legais e estatuindo penas. Conforme constata Pedro Dias Venâncio, apesar de o Código Penal desde cedo ter previsto a possibilidade da consagração de crimes praticados através de meios informáticos – de que é exemplo o artigo 221.º CP (burla informática e nas comunicações, com origem em 1995), só com a Lei da Criminalidade Informática se veio "completar de modo abrangente o leque de crimes informáticos em sentido estrito"[208]. Quanto a estes, o Autor adianta que são aqueles em que "o elemento digital surge como parte integradora do tipo legal ou mesmo como seu objeto de proteção"[209].

Em 2004 surge a Lei 41/2004, como o objetivo de transpor para a ordem jurídica nacional a Diretiva n.º 2002/58/CE[210], do Parlamento Europeu e do Conselho, de 12 de julho, que se destina à "Proteção de dados pessoais e privacidade nas telecomunicações", estabelecendo a privacidade exigida no setor das comunicações eletrónicas. Esta Lei não dispõe, tal como a Lei da Criminalidade Informática, de qualquer norma processual, aplicando-se ao "tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos de recolha de dados e de identificação" – conforme se retira do seu artigo 1.º n.º 2. Tanto a Lei como a Diretiva que aquela transpôs apenas "regulam os direitos dos utilizadores no tratamento de dados pessoais e a proteção da sua privacidade face aos prestadores de serviços"[211], e não quaisquer meios de obtenção de prova, que são o foco da presente investigação.

---

[208] Como se retira e infere de Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 21.

[209] Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 17.

[210] Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058&from=PT, acedido e consultado a 27-07-2017.

[211] Como se retira do Acórdão do Tribunal de Évora de 20 de janeiro de 2015, relator: João Gomes de Sousa, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument, acedido e consultado a 06-07-2017.

b) A Diretiva 2006/24/CE e a Lei 32/2008

Em 2008 surge a Lei 32/2008, com o objetivo de transpor para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à "conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações"[212].

Após os atentados terroristas ocorridos em 2001, 2004 e 2005 e sob a vigência da Diretiva 2002/58/CE atrás referida, dá-se a proliferação de legislação dos Estados Membros relativas à permissão ou mesmo imposição de conservação de dados de tráfego e localização pelos fornecedores de serviço, "precisamente para fins de prevenção, investigação, deteção e repressão de infrações penais"[213]. Alguns Estados impuseram a obrigação de conservação de dados autonomamente ou com fundamento no artigo 15.º[214] da Diretiva, no rescaldo do medo e insegurança vividos após os ataques terroristas, outros Estados Membros não previram qualquer obrigação de conservação dos dados aos seus fornecedores de serviços.

Neste contexto de legislações díspares na União Europeia, surge assim a Diretiva 2006/24/CE, com o objetivo declarado de harmonizar a legislação dos Estados-Membros nesta matéria: visava "harmonizar as disposições dos Estados-Membros relativas às

---

[212] Disponível em https://www.cnpd.pt/bin/legis/internacional/DIR2006-24-CE.pdf, acedido a 21-07-2017.

[213] Ramalho, David Silva, e José Duarte Coimbra. "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves." *O Direito*, 2015, ano 147: 997-1045. Página 1005.

[214] O artigo 15.º da Diretiva 2002/25/CE, com a epígrafe "Aplicação de determinadas disposições da Diretiva 95/46/CE" dispõe que: "1. Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.o e 6.o, nos n.os 1 a 4 do artigo 8.o e no artigo 9.o da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.o 1 do artigo 13.o da Diretiva 95/46/CE. **Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado**, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.o do Tratado da União Europeia. 2. O disposto no capítulo III da Diretiva 95/46/CE relativo a recursos judiciais, responsabilidade e sanções é aplicável no que respeita às disposições nacionais adotadas nos termos da presente diretiva e aos direitos individuais decorrentes da presente diretiva. 3. O Grupo de Proteção das Pessoas no que respeita ao Tratamento de Dados Pessoais, instituído nos termos do artigo 29.o da Diretiva 95/46/CE, realizará também as tarefas previstas no artigo 30.o da mesma diretiva no que respeita às matérias abrangidas pela presente diretiva, nomeadamente a proteção dos direitos e liberdades fundamentais e dos interesses legítimos no sector das comunicações eletrónicas" (negrito nosso).

obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro" – conforme o seu o artigo 1.º. A Diretiva impunha assim aos Estados Membros a adoção de legislação que previsse a obrigação de conservação dos dados de tráfego e localização pelas empresas fornecedoras de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, conservação com prazo mínimo de 6 meses e limite máximo de 2 anos – estando a fixação do quantitativo na opção de cada Estado Membro, desde que respeitados os limites temporais mínimos e máximos fixados na Diretiva.

No entanto, esta Diretiva padecia de alguns aspetos apontados como negativos[215], tal como elencam Alessandra Silveira e Pedro Freitas: "a diretiva abrangia *todos* aqueles que utilizassem serviços de comunicações eletrónicas na Europa – sem que as pessoas cujos dados eram conservados se encontrassem numa situação suscetível de dar lugar a ações penais"[216]; não estabelecia critérios objetivos relativos ao acesso das entidades nacionais aos dados, bem como da sua posterior utilização; e era ainda dúbio se existiria uma efetiva fiscalização da conservação dos dados por uma entidade independente, visto que nada na Diretiva impunha que a conservação dos dados se desse dentro do território da União. Pareciam estar em causa direitos fundamentais dos cidadãos europeus, tais como o direito à proteção da vida privada, previsto no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia, o direito à proteção de dados pessoais, previsto no artigo 8.º; e o direito à liberdade de expressão e de informação previsto no artigo 11.º, também da Carta dos Direitos Fundamentais da União Europeia.

Em 2014 o Tribunal de Justiça da União Europeia foi chamado a pronunciar-se sobre a validade desta Diretiva, cuja transposição para o ordenamento jurídico português esteve na

[215] Já apontados na Irlanda e Alemanha, que deu conta Benjamim da Silva Rodrigues em Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 391 e seguintes.

[216] Silveira, A., e P. M Freitas. "Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental." *Revista de Direito, Estado e Telecomunicações*, maio de 2017: 47-68. Página 49.

origem da Lei 32/2008, o que fez no acórdão *Digital Rights Ireland*, a 8 de abril de 2014[217]. Neste acórdão, o Tribunal de Justiça pronunciou-se no sentido da total invalidade da Diretiva.

Como constatam David Silva Ramalho e José Duarte Coimbra, esta invalidade tem como questão de fundo a inquestionável afetação da autonomia dos cidadãos europeus com a conservação dos dados de tráfego e de localização – que, apesar de não dizerem respeito ao *conteúdo* das suas comunicações eletrónicas, revelam quase tanto como aquele: permitem saber com quem se comunica, de onde, através de que meio e qual a duração da comunicação[218]. Segundo o entendimento do Tribunal de Justiça, a Diretiva padece de graves lacunas, não procedendo a limitações subjetivas quanto aos dados a conservar, nem estabelecendo limites geográficos ou temporais que estivessem relacionados com a prática de crimes graves. Assim, "da Diretiva não resultariam garantias de que a conservação e utilização de tais dados seriam feitas na estrita medida do necessário, pelo que, sem ser necessário o recurso a quaisquer outras dimensões de proporcionalidade, a Diretiva soçobraria pela sua falta de conformidade em face ao parâmetro da «necessidade»"[219 e 220].

O Tribunal de Justiça, a 21 de dezembro de 2016, voltou a pronunciar-se sobre a matéria no Acórdão *Tele2*, referente aos processos n.º C-203/15 e C-698/15, a propósito dos regimes de dois Estados Membros que transpuseram a Diretiva, Suécia e Reino Unido[221].

---

[217] Disponível em http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=PT&cid=793543, acedido a 21-07-2017.

[218] Ramalho, David Silva, e José Duarte Coimbra. "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves." *O Direito*, 2015, ano 147: 997-1045. Página 1013.

[219] Como se retira de Ramalho, David Silva, e José Duarte Coimbra. "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves." *O Direito*, 2015, ano 147: 997-1045. Página 1015.

[220] Conforme Alessandra Silveira e Pedro Freitas, o Tribunal entendeu neste sentido uma vez que "se é certo que a luta contra a criminalidade grave assume primordial importância para garantir a segurança pública – e que a sua eficácia pode depender da utilização das técnicas modernas de investigação –, tal objetivo de interesse geral por muito fundamental que seja, não pode por si só justificar que uma medida de conservação como a que foi instituída pela Diretiva 2006/24 seja necessária para os efeitos daquele combate" - conforme se retira de Silveira, A., e P. M Freitas. "Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental." *Revista de Direito, Estado e Telecomunicações*, maio de 2017: 47-68. Página 50.

[221] Disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=PT&mode=Ist&dir=&occ=first&part=1&cid=48416, acedido e consultado a 12-09-2017.

i. O Acórdão *Digital Rights Ireland* e a invalidade da Diretiva 2006/24/CE

Apenas uma palavra quanto à declaração de invalidade da Diretiva. Coloca-se a questão de saber, para além dos efeitos temporais desta invalidade[222], quais os efeitos que esta produzirá relativamente às disposições nacionais que a transpuseram – existindo já dois recursos prejudiciais para o Tribunal de Justiça dar resposta, não o tendo determinado no Acórdão *Digital Rights Ireland*. A questão tem importância para a presente investigação pois trata-se de mais um ponto dúbio relativo aos meios de obtenção de prova que se dirigem às comunicações eletrónicas, neste ponto relativo aos dados gerados por essas comunicações e não ao seu conteúdo – em que parece haver confusão generalizada, inclusive entre normativos legais.

Face à declaração de invalidade da Diretiva, a reação dos Estados Membros não foi unânime, tendo alguns Estados declarado inválidas as suas leis que transpuseram a Diretiva, e outros considerado que as exigências substanciais impostas pelo acórdão do *Digital Rights Ireland* estavam cumpridas – onde se enquadra Portugal.

Na Nota Prática n.º 7/2015 emitida pelo Gabinete de Cibercrime do Ministério Público[223], foi entendido que "a decisão de 8 de abril de 2014 não interferiu no quadro nacional vigente"[224], uma vez que a Lei 32/2008 "introduziu um mais alargado quadro, muito complexo, de regulamentação do processo de retenção de dados"[225], tendo o legislador português ido além do legislador comunitário, e satisfeito *a priori* as exigências feitas pelo acórdão do Tribunal de Justiça – o que foi alicerçado pela Reunião do *Consultative Forum*

Para mais desenvolvimentos sobre o tema, consultar a Deliberação n.º 641/2017 da Comissão Nacional da Proteção de Dados, nas suas páginas 1 a 2v, disponível em https://www.cnpd.pt/bin/decisoes/Delib/20_641_2017.pdf, consultado a 12-09-2017.

[222] Para mais desenvolvimentos sobre o tema, consultar: Silveira, A., e P. M Freitas. "Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental." *Revista de Direito, Estado e Telecomunicações*, maio de 2017: 47-68. Página 50. E Ramalho, David Silva, e José Duarte Coimbra. "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves." *O Direito*, 2015, ano 147: 997-1045. Página 1027 e seguintes.

[223] Disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_retencao_de_dados.pdf, acedido e consultado a 21-07-2017.

[224] Conforme se retira da Nota Prática n.º 7/2015 referida, ponto 3.

[225] Conforme se retira da Nota Prática n.º 7/2015 referida, ponto 5.

of Prosecutors General of the Member States of the European Union, realizada em Haia, a 11 de dezembro de 2015. De facto é de notar que "num louvável – e, de resto, incomum – exercício de transposição crítica da Diretiva, o legislador português antecipou a generalidade das omissões e insuficiências agora identificadas pelo TJ no texto comunitário e criou um diploma significativamente mais exigente"[226].

Já a Comissão Nacional de Proteção de Dados, em deliberações recentes, recomenda a revisão da Lei 32/2008, "para garantia dos direitos fundamentais à reserva da intimidade da vida privada, à inviolabilidade das comunicações e à proteção dos dados pessoais"[227], dado que a retenção de dados pessoais padece do mesmo vício da Diretiva, "traduzindo-se de tal conservação num tratamento automático de dados pessoais com risco significativo de abuso e de acesso ilícito aos mesmos"[228]. O que é desproporcional, uma vez que não se atende a "um específico indício que permita associar uma pessoa a um concreto crime, mesmo que apenas como suspeito". Assim, a 18 de julho de 2017, a Comissão Nacional de Proteção de Dados deliberou pela desaplicação da Lei 32/2008 nas situações que lhe forem submetidas a aplicação[229], sendo a Entidade a quem compete a instrução dos processos de contraordenação e aplicação de coimas relativas às condutas estabelecidas na Lei 32/2008 – o que não é de pouca importância. Resta saber qual, e quando, será a próxima tomada de posição do legislador.

Analisando a Lei 32/2008, retira-se que a lei portuguesa apenas permite a conservação e arquivo dos dados de tráfego e de localização, bem como os dados conexos necessários para identificação do assinante ou utilizador registado[230] que sejam essenciais à

---

[226] Ramalho, David Silva, e José Duarte Coimbra. "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves." *O Direito*, 2015, ano 147: 997-1045. Página 1037.

[227] Conforme se retira da Deliberação 641/2017 da Comissão Nacional de Proteção de Dados, página 2v., disponível em https://www.cnpd.pt/bin/decisoes/Delib/20_641_2017.pdf, acedida a 12-09-2017.

[228] Como se retira da Deliberação 641/2017, disponível em https://www.cnpd.pt/bin/decisoes/Delib/20_641_2017.pdf.

[229] Conforme se retira da Deliberação n.º 1008/2017, página 2, disponível em https://www.cnpd.pt/bin/decisoes/Delib/20_1008_2017.pdf, acedido a 12-09-2017.

[230] Que são elencados no artigo 4.º n.º 1 da Lei 32/2008: "a) Dados necessários para encontrar e identificar a fonte de uma comunicação;
b) Dados necessários para encontrar e identificar o destino de uma comunicação;
c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;
d) Dados necessários para identificar o tipo de comunicação;

"investigação, deteção e repressão de crimes graves" – conforme se retira do artigo 1.º n.º 1 da Lei 32/2008. Como crime grave podemos entender "crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima" – artigo 2.º n.º 1 g).

O período de preservação dos dados imposto aos fornecedores de serviços de comunicações eletrónicas é de um ano – artigo 6.º[231]. Por sua vez, "a conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de agosto, e na legislação processual penal relativamente à interceção e gravação de comunicações" – artigo 1.º n.º 2 da Lei 32/2008.

Quanto à transmissão dos dados a conservar, a Lei 32/2008 possui um regime processual próprio, desde logo consagrado nos artigos 3.º e 9.º: é necessária decisão judicial que ordene ou autorize essa transmissão às autoridades elencadas, "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", apenas podendo ser requerida pelo Ministério Público ou entidade criminal competente, e cujos dados sejam relativos a "suspeito ou arguido", a "pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido" ou a "vítima de crime, mediante o respetivo consentimento, efetivo ou presumido" – conforme se retira do artigo 9.º[232]. A Lei portuguesa prescreve ainda a destruição dos dados após o período de retenção, nos termos do artigo 7.º.

---

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
f) Dados necessários para identificar a localização do equipamento de comunicação móvel".

[231] Apesar de ter estabelecido o período máximo de conservação em metade do autorizado pela Diretiva, para que ainda assim o legislador português não previu critérios objetivos que garantissem que a conservação de dados apenas pelo período estritamente necessário – não escapando às insuficiências apontadas à Diretiva neste ponto - Como se retira e infere de Ramalho, David Silva, e José Duarte Coimbra. "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves." *O Direito*, 2015, ano 147: 997-1045. Página 1039.

[232] Está assim respeitado o requisito de prévia ordem do juiz para a divulgação dos dados, considerada fundamental pelo Tribunal de Justiça no acórdão *Digital Rights Ireland*.

Alessandra Silveira e Pedro Freitas entendem que "a declaração de invalidade das disposições normativas constantes de uma diretiva europeia afeta inelutavelmente o ato legal de transposição da mesma para o ordenamento jurídico interno" e que "um Estado-Membro não pode utilizar a faculdade conferida pelo artigo 15.º n.º 1 da Diretiva 2002/58 para impor a manutenção de uma obrigação geral de conservação de dados na sequência da declaração de invalidade da Diretiva 2006/24"[233], invocando o princípio da lealdade europeia (previsto no artigo 4.º n.º 3 do Tratado da União Europeia), o princípio da igualdade e não discriminação em razão da nacionalidade (previsto no artigo 18.º do Tratado de Funcionamento da União Europeia) – uma vez que nos Estados Membros em que se continua a aplicar a legislação que transpôs a Diretiva podem existir condenações penais que tiveram por base o acesso aos dados conservados, e ainda a força juridicamente vinculativa das decisões do Tribunal de Justiça da União Europeia[234].

Por sua vez David Ramalho e José Duarte Coimbra consideram que o juiz de instrução não pode ordenar a produção de prova com base em dados de tráfego conservados ao abrigo da Lei 32/2008, "por se tratar de um órgão jurisdicional e, por essa razão, integralmente sujeito aos efeitos do primado, nenhum juiz pode *aplicar* ou *fazer aplicar* a Lei 32/2008, de 17 de julho, a qual se revela, após o dia 8 de abril de 2014, em estado de verdadeira latência"[235]. Assim, apesar de formalmente vigente, trata-se de um diploma cuja eficácia é dúbia, pois possui medidas frontalmente contrárias ao Direito da União Europeia.

ii. A Lei 32/2008, o artigo 189.º n.º 2 CPP e a Lei do Cibercrime

Ultrapassando a querela pendente da (in)validade da Lei 32/2008 e por dever de análise académica, por não haver ainda posição definida pelo legislador comunitário nem

[233] Silveira, A., e P. M Freitas. "Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental." *Revista de Direito, Estado e Telecomunicações*, maio de 2017: 47-68. Página 52.

[234] Conforme se retira de Silveira, A., e P. M Freitas. "Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental." *Revista de Direito, Estado e Telecomunicações*, maio de 2017: 47-68. Página 52 e seguintes.

[235] Ramalho, David Silva, e José Duarte Coimbra. "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves." *O Direito*, 2015, ano 147: 997-1045. Página 1042.

ação dos Tribunais Portugueses junto do Tribunal de Justiça para esclarecer a questão, é de notar que o regime processual de conservação e transmissão dos dados conservados previsto na Lei 32/2008 possui requisitos bastante similares aos das escutas telefónicas, tanto no catálogo de crimes como nos apertados requisitos para a sua possível transmissão.

Para além disso, prevê o artigo 189.º n.º 2 do CPP que: "A **obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações** só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo" (negrito nosso). Assim, com a entrada em vigor da Lei 32/2008, colocava-se a questão de saber se esta não teria retirado algum do substrato a que se referia o artigo 189.º n.º 2 do CPP – nomeadamente quanto aos dados de localização e de tráfego gerados pelas comunicações eletrónicas[236], cujo acesso e tratamento pela investigação criminal o legislador continua, ainda hoje, a estender ao regime das escutas telefónicas[237].

Para Conde Correia, visto que os requisitos para a transmissão dos dados de tráfego e localização e os das escutas telefónicas são essencialmente os mesmos, faz com que esta duplicação de regimes no Código de Processo Penal e na Lei 32/2008 tenha sido desacompanhada de qualquer "razão técnica válida", sendo que "o legislador podia (e devia) ter mantido a centralidade normativa do Código de Processo Penal"[238], não sendo necessário ter-se autonomizado o meio de obtenção de prova em legislação avulsa, considerando que "apenas o que é técnico ou acessório deveria estar consagrado no regime especial, tendo o restante inequívoca dignidade processual penal"[239 e 240].

---

[236] No mesmo sentido se conclui no Acórdão do Tribunal de Évora de 20 de janeiro de 2015, relator: João Gomes de Sousa, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument, acedido e consultado a 06-07-2017.

[237] Apesar de não ser o objeto do nosso estudo, não poderíamos furtar-nos a uma referência a este aspeto, pois é (mais) um exemplo flagrante da possibilidade de esvaziamento do artigo 189.º CPP.

[238] Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 33.

[239] Como se retira de Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 33.

[240] Quanto à questão da compatibilidade entre o artigo 189.º CPP e a conservação de dados de tráfego e de localização, consultar entendimento do Tribunal de Évora de 25 de outubro de 2016, Como se retira do Acórdão do Tribunal de Évora de 25 de outubro de 2016, relator: João Gomes de Sousa, disponível em:

Cabe ainda dizer que com a entrada em vigor da Lei do Cibercrime se colocou a questão de saber se os artigos 3.º n.º 1 e 9.º n.º 1 e 3 da Lei 32/2008 não teriam sido revogados. Quanto a esta questão, pronunciaram-se os Acórdãos do Tribunal de Évora de 6 e 20 de janeiro de 2015: "admitindo que todo o diploma de 2008 está em vigor na parte «arquivística», que sem dúvida está, o que concretamente se deve afirmar é que os artigos 3.º n.º 1 e 9.º n.º 1 e 3 da citada Lei foram revogados pelo regime processual penal para dados informáticos contido nos artigos 11.º a 19.º da Lei n.º 109/2009"[241], sendo a Lei 32/2008 "um diploma que regula arquivos"[242], estando a parte "arquivística" do diploma em vigor, bem como o que diz respeito aos dados contidos no artigo 4.º n.º 1 da Lei. Importante é notar que em momento algum o Tribunal, num ou noutro acórdão, tomou em consideração o Acórdão *Digital Rights Ireland* e a questão da possível invalidade da Lei 32/2008: considerou que esta se mantém plenamente em vigor na matéria de conservação de dados de tráfego e de localização. Este facto revela, no mínimo, a desconsideração da *praxis* pela problemática atrás explanada, e ainda alguma confusão quanto ao âmbito de aplicação das leis em causa – Lei 32/2008 e do Cibercrime. É mais um caso em que é exigido ao intérprete e aplicador um esforço acrescido na determinação do âmbito de aplicação do artigo 189.º, agora do seu número 2, devido às Leis avulsas que foram sendo consagradas, e que por vezes não possuem soluções consentâneas entre si[243].

---

http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/8a62944fb55a34c580258057004f3f1d?OpenDocument, acedido e consultado a 28-07-2017: "o artigo 189.º do CPP nunca é aplicável à prova das comunicações conservadas em sistemas informáticos nos termos da Lei 32/2008. Dito de outra forma, o regime das escutas do Código de Processo Penal nunca é aplicável por extensão aos dados abrangidos pela Lei 32/2008".

[241] Como se retira do Acórdão do Tribunal de Évora de 20 de janeiro de 2015, relator: João Gomes de Sousa, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument, acedido e consultado a 06-07-2017.

[242] Como se retira do Acórdão do Tribunal de Évora de 6 de janeiro de 2015, relator: João Gomes de Sousa, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument, acedido e consultado a 06-07-2017.

[243] Que, por economia do presente trabalho, não poderemos dar conta. Para mais desenvolvimentos sobre o tema e análise das diferentes posições sobre a matéria, consultar: Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 36. E ainda a Nota Prática n.º 8/2016 do Gabinete do Cibercrime do Ministério Público, disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_pedido_de_info_a_isp.pdf, acedido e consultado a 27-07-2017. Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 117 e seguintes e Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 280 e seguintes. Albuquerque, Paulo Pinto de. *Comentário do Código de Processo Penal à luz da Constituição da República*

c) A Convenção sobre o Cibercrime e a Lei 109/2009

A Convenção sobre o Cibercrime é um tratado de direito internacional sobre a cibercriminalidade contra sistemas de computadores, redes e dados, aberta à assinatura dos diversos países a 23 de novembro de 2001, assinada por Portugal nessa mesma data e ratificada em 2009. No seu seguimento foi publicada a Lei do Cibercrime – Lei 109/2009[244], que veio ao mesmo tempo transpor para a ordem jurídica a Decisão-Quadro nº 2005/222/JAI, do Conselho[245][246].

A Convenção sobre o Cibercrime, promovida pelo Conselho da Europa, tinha no seu reduto três objetivos principais: "pretende harmonizar legislações e os crimes nela previstos; pretende estender às jurisdições de Estados Parte determinados instrumentos processuais e de produção de prova modernos e adequados à investigação da cibercriminalidade; por último, pretende facilitar a cooperação internacional e viabilizar investigações"[247]. Os mesmos objetivos prosseguiu a Decisão-Quadro nº 2005/222/JAI, impondo aos Estados-Membros da União Europeia uma abordagem comum à problemática da criminalidade informática e cooperação.

Como se constata no Acórdão do Tribunal de Évora de 20 de janeiro de 2015, em que foi relator o Dr. João Gomes de Sousa, "só em 15 de setembro de 2009 – quase oito anos e só após a revisão do CPP – esta Convenção será aprovada pela Resolução da Assembleia da República n.º 88/2009, ratificada pelo Decreto Presidencial n.º 91/2009 e publicada naquela

---

Portuguesa e da Convenção Europeia dos Direitos do Homem. 4ª edição. Universidade Católica, 2011. Página 549 e Cabral, José António Henriques dos Santos, António Pires Henriques da Graça, António Henriques Gaspar, Eduardo Maia Costa, António Jorge de Oliveira Mendes, e António Pereira Madeira. *Código de Processo Penal Comentado.* Almedina , 2014. Página 837.

[244] Através da Resolução da Assembleia da República n.º 88/2009 e Decreto do Presidente da República n.º 92/2009, publicados a 15 de Setembro – como se retira de Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011. Página 21.

[245] Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222, acedido e consultado a 01-05-2017.

[246] Quanto ao processo legislativo do "Pacote de Leis sobre o Cibercrime", consultar Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 100 e seguintes.

[247] Verdelho, Pedro. *A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa.* Vol. VI, em *Direito da Sociedade da Informação*, de AA. VV., 257-277. Coimbra Editora, 2006. Página 258.

data, no mesmo Diário da República que igualmente acolheu a publicação da Lei 109/2009 (…)"[248].

Em 2009, com a Lei do Cibercrime, o legislador, tal como antevia Pedro Verdelho em 2004[249], "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 as regras gerais do Código de Processo Penal) e ainda normas respeitantes à cooperação penal internacional"[250]. Apesar de terem sido mantidas disposições dispersas atinentes à utilização de sistemas informáticos, que podem causar confusão na aplicação das Leis – de que é exemplo a Lei 32/2008 e o artigo 189.º CPP, de que já demos conta.

Com a Lei do Cibercrime, o legislador tipificou vários crimes cuja consagração foi considerada essencial no espaço europeu e internacional para o combate da cibercriminalidade – por definição, global e transfronteiriça; e ainda criou diversos meios de obtenção de prova, como a preservação expedita de dados (artigo 12.º) e a sua revelação (artigo 13.º), a injunção para apresentação ou concessão do acesso a dados (artigo 14.º), pesquisa de dados informáticos (artigo 15.º) e a sua apreensão (artigo 16.º), e a apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17.º) que se dirigem a este específico setor de atividade, e ainda os "cometidos por meio de sistema informático" ou "em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico" – artigo 11.º LC. Para além destes meios de obtenção de prova, foram ainda

[248] Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument, acedido e consultado a 06-07-2017.

[249] Já em 2004, Pedro Verdelho entendia que o legislador português, quando procedesse às alterações legislativas impostas pela adaptação da Convenção, poderia ter de escolher uma de entre duas alternativas: "ou altera pontualmente os vários diplomas legislativos que tratam as matérias a que se refere o articulado da Convenção ou elabora uma lei nova que derrogue parcialmente todos aqueles diplomas e regulamente globalmente a matéria (uma espécie de Código da Criminalidade Informática, incluindo disposições de direito penal substantivo, de direito processual penal e ainda de cooperação judiciária internacional)", entendendo que a opção mais coerente com a tradição legislativa portuguesa seria a elaboração de um código sectorial, com a vantagem da sistematização de todos os normativos adstritos a um específico setor de criminalidade, eliminando assim regras especiais de outros normativos penais estruturantes, o que facilitaria a prática judiciária – como se retira de Verdelho, Pedro. *A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa.* Vol. VI, em *Direito da Sociedade da Informação*, de AA. VV., 257-277. Coimbra Editora, 2006. Página 276.

[250] Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Iuridica*, Outubro-Dezembro de 2009, n.º 320. Página 719.

criados, pela Lei do Cibercrime, a interceção de comunicações (artigo 18.º) e as ações encobertas (artigo 19.º), de cujos normativos consta o catálogo de crimes a que são aplicáveis.

Tal como deixamos antever no capítulo anterior, permanecem ainda hoje alguns nódulos problemáticos no Código Penal e de Processo, nomeadamente nos artigos 193.º e 194.º CP, cujo conteúdo foi esvaziado através dos crimes consagrados na Lei do Cibercrime, bem como do artigo 189.º n.º 1 CPP com alguns dos meios de obtenção de prova consagrados na Lei do Cibercrime, de que daremos conta infra. A tudo isto acresce a constatação do "desprezo da praxis" ainda hoje quanto à Lei do Cibercrime, "que apenas é explicável pelo efeito de atração, quase hipnótico e excludente, que é exercido sobre o intérprete pelos artigos 187.º a 190.º do CPP"[251].

6. O artigo 189.º CPP – "casa dos horrores hermenêutica"?

Ciente da nova realidade sociológica e comunicacional que se afirmou desde o aparecimento da Internet, tem-se assistido a um esforço legislativo de adequação da lei adjetiva às práticas comunicacionais atuais e ao desenvolvimento tecnológico verificado desde os anos 80: que permitiram o aparecimento de novos meios de obtenção de prova, ao "lado" dos meios tradicionais, bem como novos meios de comunicação e até novos tipos de criminalidade – em que se recorre à tecnologia e informática para cometer crimes.

Assim, num primeiro momento o legislador optou pela extensão do regime das escutas telefónicas à interceção das conversações realizadas por meio diferente do telefone, nomeadamente o "correio eletrónico e outras formas de transmissão de dados por via

[251] Tal como foi constatado no Acórdão do Tribunal de Évora de 20 de janeiro de 2015, relator: João Gomes de Sousa, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument, acedido e consultado a 06-07-2017. Tratou-se de um processo em que, para a recolha para a investigação criminal de dados de tráfego e de localização celular, se recorreu ao normativo do artigo 189.º n.º 2 do CPP, sem ter em consideração as disposições da Lei 32/2008 nem a Lei do Cibercrime, em vigor.
No mesmo sentido entende Conde Correia, considerando que há na *praxis* jurídica abundantes exemplos de falta de coordenação do Código Penal, da Lei do Cibercrime e da Lei 32/2008 – como se retira de Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 35.

telemática", mesmo que essas conversações se encontrem armazenadas em suporte digital, indo ainda mais longe, estendendo o regime também às conversações entre presentes[252] – plasmado no artigo 189.º nº 1 CPP. Ao longo do tempo o legislador foi criando legislação avulsa que disciplina setores da "criminalidade informática sem sentido amplo", e mesmo após a criação da Lei do Cibercrime, em 2009, que consagrou meios de obtenção de prova específicos para o setor da cibercriminalidade, e ainda para qualquer crime em que exista o recurso a meios tecnológicos, o legislador não procedeu a qualquer alteração ao artigo 189.º CPP – sendo de questionar qual a sua aplicabilidade prática, para além da confusão normativa que gera.

Conforme ensina Paulo Pinto de Albuquerque, o Código de Processo Penal, na sua versão originária, "consagrava um princípio de que a palavra dita merece mais proteção do que a palavra escrita" [253] – resultando por isso que a apreensão de documentos seja um meio de obtenção de prova admissível em relação a qualquer crime, ao passo que a utilização das escutas telefónicas apenas possa ser aplicável a um catálogo de crimes estabelecido pelo legislador, considerados como mais graves. Ao que acresce que a apreensão de correspondência apenas pode ter lugar se respeitados os requisitos do artigo 179.º CPP: em investigações cuja causa seja "crime punível com pena de prisão superior, no seu máximo, a 3 anos" e que "a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova". No entanto, como constata o ilustre Autor, o princípio segundo o qual a palavra dita mereceria maior proteção do que a palavra escrita tem "sofrido uma progressiva erosão desde 1998, notando-se uma clara tendência para o alargamento do âmbito de aplicação do regime de proteção da palava dita"[254] – como facilmente se constata pela extensão da

[252] É este mais um nódulo problemático do artigo 189.º n.º 1 CPP, que por economia do presente trabalho e delimitação temática não nos pode ocupar. Para mais desenvolvimentos sobre o tema, consultar: Manuel da Costa Andrade, *"Bruscamente no Verão Passado", a reforma do Código Processual Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009, página 162 e seguintes; João Gouveia de Caires, "O registo de Som e Imagem e as Escutas Ambientais", *Direito da Investigação Criminal e da Prova*, Almedina, 2014, página 283 e seguintes; Paulo Pinto de Albuquerque, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª Edição, Universidade Católica, 2011, página 546, nota 11 e seguintes; entre outros.

[253] Albuquerque, Paulo Pinto de. *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* 4ª edição. Universidade Católica, 2011. Página 542.

[254] Albuquerque, Paulo Pinto de. *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* 4ª edição. Universidade Católica, 2011. Página 542.

proteção conferida à palavra falada e ao e-mail (e às restantes formas de comunicação eletrónica), que se processam como comunicações escritas.

Paulo Pinto de Albuquerque considera, perante as sucessivas alterações legislativas e ampliação do leque de realidades a que se aplica o regime das escutas telefónicas, que o legislador "criou uma total inconsistência no sistema dos meios de obtenção de prova, havendo atualmente objetos de registo da palavra escrita (telegrama, fax, telex) sujeitos ao regime geral das apreensões (artigo 178.º) quando o seu conteúdo é conhecido pelo seu destinatário e sujeitos a um regime especial de apreensão (artigo 179.º) quando o seu conteúdo é ainda desconhecido pelo seu destinatário e ainda objetos de registo da palavra escrita (os referidos suportes materiais de correio eletrónico ou de outras formas de transmissão de dados por via telemática) submetidos ao regime das escutas telefónicas, independentemente do seu conteúdo ser já conhecido ou não pelo seu destinatário"[255].

Como conclui Costa Andrade, o legislador trata de igual forma "constelações pertinentes a três categorias distintas: a intromissão nas telecomunicações, o acesso aos «documentos» guardados no computador e que resultarem de comunicações eletrónicas, e gravações de conversações entre presentes"[256 e 257].

Conforme Paulo Dá Mesquita, esta opção sistemática de extensão do regime das escutas telefónicas acentua a descaracterização deste instituto, uma vez que abrange as comunicações que se encontrem armazenadas em suporte digital – e, como tal, já não podem ser consideradas comunicações, mas os seus suportes. Este Autor entende que se tratou de uma inovação teleologicamente infundada e ainda imprecisa "por carência de explicitação de um critério delimitador entre o âmbito de proteção das comunicações teleologicamente cobertas pelo manto da norma (o próprio conceito de comunicação não se cinge, no plano

[255] Albuquerque, Paulo Pinto de. *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* 4ª edição. Universidade Católica, 2011. Página 542.

[256] Manuel da Costa Andrade, *"Bruscamente no Verão Passado", a reforma do Código Processual Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009. página 185.

[257] Já Francisco Marcolino de Jesus entende que a extensão envolve cinco dimensões: (1) do telefone a outros meios técnicos; (2) da voz humana à imagem; (3) da comunicação à distância à comunicação entre presentes; (4) da ingerência (no conteúdo das) nas conversações ou comunicações à obtenção do registo de realização das mesmas; (5) da ingerência «transambiental» à localização geográfica do aparelho técnico da comunicação" – como se retira de Jesus, Francisco Marcolino de. *Os meios de obtenção de prova em Processo Penal.* 2ª - Reimpressão. Almedina, 2015. Página 319.

epistemológico, à comunicação através de redes eletrónicas), essencial para identificar a autonomia de dados *guardados* em suporte digital que tenham sido transmitidos no passado (ou seja um ficheiro informático que guarde dados relativos a comunicações interpessoais pode derivar de prévias transmissões através de redes eletrónicas ou não)"[258].

Já em 2008, Benjamim da Silva Rodrigues considerava que "o paradigma da ponderação constitucional" exigido para a intervenção em conversações que se processassem através de chamadas, levadas a cabo por telefone ou qualquer outro meio técnico "foi desvirtuado «por extensão» passando a abranger-se, neste meio de obtenção de prova, situações que, pela sua natureza, mereceriam a consagração de um regime autónomo e diferenciado"[259] – autonomização viria a dar-se, no que toca à prova eletrónica pelo menos, fora do Código do Processo Penal – com a Lei do Cibercrime[260]. No que toca à exceção do regime do regime das escutas telefónicas ao correio eletrónico e a outras formas de transmissão por via telemática e às comunicações entre presentes, aponta o Autor como crítica o facto de o artigo 189.º CPP ser "uma norma excecional de extensão (excecional) do regime das escutas telefónicas a outros meios a ele equiparados, pelo que efetuar uma segunda extensão dentro do âmbito da excecionalidade é algo de inconcebível ao nível da metódica constitucional de restrição de direitos constitucionalmente consagrados e tutelados no artigo 34.º n.º 1 e 4 da CRP de 1976"[261].

Passemos à tentativa de compreensão de quais são, afinal, os meios de obtenção de prova que se dirigem à ingerência nas comunicações eletrónicas – tendo em mente que se podem dar por via escrita, oral, ou ambas, e que essa ingerência se pode dar em tempo real, ou póstumo, através do acesso a ficheiros e dados informáticos.

[258] Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 90.
[259] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 427.
[260] Tal como entende Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 98.
[261] Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 128.

Capítulo IV – A ingerência no conteúdo das comunicações eletrónicas pela investigação criminal

> "A teia legislativa nacional é muito complexa, sobrepondo-se em camadas sucessivas, que ora parecem divergir e ganhar autonomia, ora parecem convergir e superar-se sucessivamente, tornando quase impossível a tarefa do melhor intérprete. As peças do *puzzle* não se encaixam facilmente."[262]
>
> João Conde Correia

1. As comunicações eletrónicas

As comunicações eletrónicas são objeto da Lei 5/2004, de 10 de fevereiro, que "estabelece o regime jurídico aplicável às redes e serviços de comunicações eletrónicas e aos recursos e serviços conexos e define as competências da autoridade reguladora nacional neste domínio, no âmbito do processo de transposição das Diretivas 2002/19/CE, 2002/20/CE e 2002/21/CE, todas do Parlamento Europeu e do Conselho, de 7 de Março.

Apesar de não adiantar uma definição de "comunicações eletrónicas", esta Lei define a "rede de comunicações eletrónicas" como "os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos, nomeadamente elementos de rede que não se encontrem ativos, que permitem o envio de sinais por cabo, meios radioelétricos, meios óticos, ou por outros meios eletromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, os sistemas de cabos de eletricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes de radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida" – artigo 3.º dd). Por "serviços de comunicações eletrónicas" define como "o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de

[262] Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 30.

redes de comunicações eletrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão, sem prejuízo da exclusão referida nas alíneas a) e b) do n.º 1 do artigo 2.º" – artigo 3.º ff).

Assim, podemos concluir que as comunicações eletrónicas integram os serviços de telefone fixo, telefone móvel, internet fixa, internet móvel e televisão, bem como redes de radiodifusão[263]. Como constata Armando Dias Ramos, "no futuro aguardam-se novas formas de comunicação. Ainda que a escrita continue a vigorar antecipa-se que esta será *residual*, dando-se prioridade às mensagens faladas, isto é, às comunicações *face-to-face* (videoconferências, *stream* de vídeos, mensagens eletrónicas de áudio e vídeo, entre outras)"[264].

As comunicações eletrónicas sob análise na presente investigação serão as chamadas realizadas através do sistema *Voice Over IP*, as mensagens instantâneas enviadas e recebidas através de aplicações informáticas que têm por base a Internet, como o *WhatsApp* e o *Messenger*, o correio eletrónico e as mensagens *SMS* e *MMS* constantes de cartões *SIM* e do armazenamento dos telemóveis.

2. A evolução legislativa no ordenamento português

O legislador português optou, desde a versão originária do Código de Processo Penal de 1987, por consagrar como modelo e exemplo paradigmático dos meios de obtenção de prova relativo à ingerência nas comunicações as escutas telefónicas. Assim, estendeu o seu regime a outros meios de obtenção de prova que se destinam a realidades bastante distintas das escutas de chamadas telefónicas, tais como a "interceção" e "leitura" de correio eletrónico ou quaisquer dados transmitidos através de via telemática, mesmo que se encontrem guardados em suporte digital ou em qualquer aparelho com essa capacidade, e até mesmo a escuta – ou visualização? – de conversações entre presentes.

[263] Conforme se retira da definição de comunicações eletrónicas adiantada pela Autoridade Nacional de Comunicações – ANACOM, em http://www.anacom-consumidor.com/-/servico-de-comunicacoes-eletronicas, acedido a 31-07-2017.
[264] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 168.

No entanto, ao fazê-lo, e subscrevemos por inteiro a opinião de Costa Andrade, o legislador converteu o artigo 189.º CPP numa "casa de horrores hermenêutica", pois "confunde o inconfundível, cria desequilíbrios inexplicáveis e submete ao mesmo regime coisas completamente heterogéneas e centrífugas, que só poderiam reclamar tratamentos diferenciados"[265]. É de notar que o legislador, através deste artigo[266], destina a aplicação do regime das escutas telefónicas tanto à "escuta" da palavra falada como à "leitura" da palavra escrita, ao submeter ao seu regime a interceção de correio eletrónico e mensagens instantâneas trocadas através de aplicações informáticas. Ao fazê-lo, afasta-se por isso do fundamento das escutas telefónicas: a palavra falada no âmbito das telecomunicações, cuja volatilidade e falta de suficiente reflexão justifica a proteção reforçada que a interceção destas conversações impõe, de que é reflexo a consagração constitucional de proteção específica da palavra falada.

Todo este imbróglio legislativo adquiriu uma nova dimensão quando o legislador, em 2009, criou meios de obtenção de prova na Lei do Cibercrime, como por exemplo a "pesquisa" e "apreensão de dados informáticos" (artigos 15.º e 16.º da LC), a "apreensão de correio eletrónico e registos de comunicações de natureza semelhante" (artigo 17.º da LC), e a "interceção de comunicações" (artigo 18.º da LC), tendo tornado dúbios os campos de aplicação de uns e outros meios de obtenção de prova, e quais as diferenças entre eles. Impõe-se assim a questão de saber qual é, ou quais são, o regime ou regimes que se destinam à "interceção"/ingerência no conteúdo das diversas comunicações eletrónicas.

Passemos à análise dos diferentes tipos de comunicações eletrónicas, tentando descortinar qual será, afinal, o regime aplicável a cada qual – partindo a investigação da análise do regime aplicável ao correio eletrónico, em que existe solução consagrada (mas não menos dúbia) e maior reflexão doutrinal e jurisprudencial sobre a mesma.

---

[265] Manuel da Costa Andrade, *"Bruscamente no Verão Passado", a reforma do Código Processual Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, 2009, página 185.

[266] Francisco Marcolino de Jesus entende que a extensão operada pelo artigo 189.º CPP projeta-se em "cinco dimensões: (1) do telefone a outros meios técnicos; (2) da voz humana à imagem; (3) da comunicação à distância à comunicação entre presentes; (4) da ingerência (no conteúdo das) nas conversações ou comunicações à obtenção do registo de realização das mesmas; (5) da ingerência «transambiental» à localização geográfica do aparelho técnico da comunicação" – como se retira de Jesus, Francisco Marcolino de. *Os meios de obtenção de prova em Processo Penal.* 2ª - Reimpressão. Almedina, 2015. Página 319.

3. O correio eletrónico

a) Considerações introdutórias

O correio eletrónico, conforme o artigo 2º f) da Diretiva 2002/58/CE[267] e o artigo 2.º n.º 1 b) da Lei 41/2004 que o reproduz, consiste em "qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário a recolher".

Para Armando Dias Ramos, o correio eletrónico é "um programa informático que permite a comunicação instantânea, de modo diferido, entre quem a envia e quem a recebe, através de redes de informação e comunicação, independentemente do local em que estes se encontrem, sem a necessidade deste se encontrar instalado no computador"[268].

Por sua vez, Benjamim da Silva Rodrigues define-o como "um fluxo informacional e comunicacional digital, sob o formato de texto, voz, som, imagem ou gráfico, que é colocado por um assinante ou consumidor de redes ou serviços de comunicações eletrónicas acessíveis ao público, no âmbito de um ciclo informacional e comunicacional (tendencialmente) fechado, através de um ponto terminal da rede, na rede pública de comunicações eletrónicas, conduzida até ao servidor de mail ou ao terminal do destinatário do fluxo até que o mesmo proceda à sua recolha, leitura e/ou posterior eliminação"[269].

Conforme o artigo 2.º n.º 1 a) da Lei 41/2004, a Lei de Proteção de Dados Pessoais e Privacidade nas Telecomunicações, o correio eletrónico cabe assim na definição de comunicação eletrónica, pois trata-se de "qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações eletrónicas acessível ao público" – definição que, aliás, inclui diversas operações informáticas que em nada são comparáveis a comunicação, como o acesso a páginas de Internet. Podemos dizer

[267] Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058&from=PT, consultado a 03-01-2017.
[268] Como se retira de Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 31.
[269] Como se retira de Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 444.

que o correio eletrónico é uma forma específica de comunicação eletrónica, consolidada na vida dos cidadãos e que se assemelha à correspondência tradicional na sua essência – enquanto mensagem a ser transmitida –, não fora a diferença de meio por que se transmite e a diversidade técnica do seu conteúdo: os anexos, em vez de documentos impressos, fotografias ou quaisquer outros elementos físicos, podem ser imagens virtuais, sons, hiperligações ou qualquer ficheiro informático.

O correio eletrónico afirmou-se, com o decorrer dos tempos e avanços tecnológicos[270], como uma forma de comunicação expedita e económica, assumindo-se desde cedo como fundamental no dia-a-dia dos indivíduos, quer na sua vida profissional como pessoal. Atualmente, quase todas as pessoas possuem, pelo menos, uma conta de *e-mail*, seja por imposições profissionais, comodidade ou necessidade de possuir uma "identidade virtual" que permita o acesso ao ciberespaço. É importante referir que nos referimos aos serviços designados por *Webmail*[271], tal como o *Gmail*, o *Hotmail*, *Yahoo*, entre outros.

Conforme ensina Paulo Dá Mesquita, o conceito de correio eletrónico é "amplo, abrangendo tanto os sistemas que utilizam o conglomerado de redes eletrónicas de escala mundial (*internet*) e são baseados no protocolo *SMTP* (*Simple Mail Transfer Protocol*), como sistemas de redes de computadores privadas (conhecidas como *intranets*), que funcionam como uma pequena rede eletrónica confinada a uma organização permitindo a troca de mensagens dentro da mesma, normalmente, baseada em protocolos próprios"[272].

Com a afirmação do correio eletrónico como forma de comunicação, a investigação criminal viu-se confrontada com os benefícios que poderiam ter o acesso e tratamento da informação gerada através desta "nova" forma de comunicação, tanto quanto ao seu conteúdo

[270] Para mais desenvolvimentos sobre a origem do correio eletrónico, consultar Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 27 e seguintes.
[271] Tal como ensina Armando Dias Ramos, "*Webmail* é um *interface* que permite, a partir de um *browser* de acesso à Internet, consultar e enviar mensagens de correio eletrónico. A maior vantagem do *webmail* é o facto de o seu utilizador não necessitar de ter instalado no seu equipamento um programa específico para a leitura ou envio de correio eletrónico, sendo apenas necessário um computador ou outro dispositivo móvel ligado à internet. Isto também significa que ao contrário de outros métodos de consulta do correio eletrónico, não é necessário utilizar sempre o mesmo computador" – como se retira de Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 28, nota 9.
[272] Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 121.

como aos dados informáticos gerados pelas mesmas. Assim, desde 1998 que o legislador português pretendeu incorporar a "vertigem tecnológica" nos meios de obtenção de prova, estabelecendo que a interceção do correio eletrónico ou de outras formas de transmissão de dados por via telemática passaria a subsumir-se expressamente ao regime das escutas telefónicas, pela mão do então artigo 190.º e atual 189.º CPP – permanecendo a consagração, com mais aditamentos, até aos dias de hoje no Código de Processo Penal.

Analisando a realidade que se pretende alcançar com a investigação criminal – o conteúdo possível do correio eletrónico (e não os dados informáticos gerados pela sua utilização e acesso[273]) cabe uma primeira palavra, relativa à sua natureza: o *e-mail* trata-se de uma forma de comunicar escrita, podendo inclusivamente ser composta por diferentes ficheiros, imagens ou sons, que se afasta da tradicional carta pela sua virtualidade (enquanto não é impressa). Talvez por este último aspeto, de se afastar da materialidade da tradicional correspondência, o legislador tenha optado, em 1998, por enquadrar a interceção do correio eletrónico no âmbito do regime que, a seu ver, era o adequado para regular a "nova realidade" cibernética, a que destinou o regime das escutas telefónicas. Talvez por esse motivo se tenha afastado do regime da apreensão de correspondência, e considerado que o melhor método para a obtenção deste "novo" tipo de prova seria o regime das escutas telefónicas, a que destinou as realidades eletrónicas.

O correio eletrónico trata-se de uma realidade complexa – a que nos parece que o legislador tem dedicado alguma atenção, mas em que ainda subsistem nódulos problemáticos: a redação e manutenção (com algumas oportunidades de alteração perdidas) dos artigos constantes do Código Processo Penal, que remetem a ingerência no correio eletrónico, sem mais, para o regime das escutas, levanta a questão de compatibilização entre o Código de Processo Penal e os meios de obtenção de prova constantes da Lei do Cibercrime, nomeadamente o que se destina especificamente à apreensão de correio eletrónico armazenado em sistemas informáticos, no decurso de pesquisas ou acesso aos mesmos – artigo 17.º LC, e ainda (quanto à possibilidade de aplicação do) ao meio de

[273] Os dados de base e de tráfego, que possuem exponencial valor para a investigação criminal, dado que podem permitir com grande precisão a localização dos indivíduos e fazer o *tracking* dos seus movimentos, quer informáticos quer físicos, e ainda estabelecer conexões entre redes e pessoas, mas que por economia do presente trabalho não nos poderemos debruçar.

obtenção de prova previsto no artigo 18.º da LC, a "interceção de comunicações", relativa à monitorização em tempo real do correio eletrónico enviado e recebido.

b) O artigo 189.º n.º 1 Código de Processo Penal

Como já exaustivamente referido, o artigo 189.º n.º 1 CPP, ainda à presente data, dispõe que: "O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital".

Armando Dias Ramos considera que esta foi uma "boa opção do legislador": "pese embora se trate de meios comunicacionais diferentes, e na falta de um regime específico para as comunicações eletrónicas, este é sem dúvida a melhor opção, sem o qual ficaríamos com um vazio legislativo, que seria um autêntico paraíso para o mundo do cibercrime. E, aqui sim, verifica-se algum paralelismo com o regime das escutas telefónicas, porquanto a ação que se vai realizar é, na pura aceção da palavra, uma verdadeira interceção da comunicação e nunca uma apreensão de comunicações"[274]. No entanto, e com o devido respeito pela opinião descrita, não é verdade que sem o artigo 189.º n.º 1 CPP, pelo menos desde 2009, se ficaria numa situação de vazio legislativo relativamente à recolha do correio eletrónico para a investigação criminal: estão consagrados na Lei do Cibercrime meios de obtenção de prova que permitem a recolha do correio eletrónico, nos casos que serão analisados *infra* – sem ser necessária a extensão operada pelo legislador no Código de Processo Penal para o regime das escutas telefónicas. Mesmo que a solução da Lei do Cibercrime fosse essa, quanto mais não o sendo, como veremos adiante.

Entendendo as escutas telefónicas no seu sentido tradicional – a audição secreta de comunicações telefónicas, trata-se da ingerência em tempo real nas comunicações, dado que as conversas se esgotam no momento em que são ditas as palavras: não há o elemento literal

[274] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 59.

que permita a perenidade (quanto muito, temporária) do que foi dito. A não ser, claro, que um terceiro se introduza na conversação e a grave.

Por sua vez, o correio eletrónico é uma forma de comunicação que passa por diversos momentos na sua concretização: desde o seu envio e trânsito na rede até chegar ao terminal do destinatário, o momento em que o *e-mail* é aberto e lido pelo mesmo e o momento em que, depois de lido, é arquivado no sistema informático[275] (ou impresso em papel) – em que deixa de ser comunicação no verdeiro sentido da palavra, contendo apenas registo da mesma. Neste sentido, apenas é possível configurar-se a "interceção" do correio eletrónico em tempo real enquanto ele transita na rede até ao terminal de destino – assim entende Rita Castanheira Neves: "Na verdade, se analisarmos a realização empírica deste meio de obtenção de prova [escutas telefónicas], percebemos que temos na sua base a captação, interceção e monitorização de mensagens que estão em pleno processo de transmissão, sendo, por isso mesmo, comunicações em curso com simultaneidade de declarações entre emissor e recetor. O correio eletrónico, por sua vez, embora importando sempre um emissor e um recetor (mínimo de dois IP) configura-se como uma mensagem – quer em texto, gráfico, animação, filme ou cálculo – que circula desde aquele primeiro até ao recetor ou recetores não havendo simultaneidade entre a emissão da comunicação e a receção do teor comunicacional dentro do mesmo (e único) processo comunicacional"[276] – sendo apenas neste momento que se pode processar a interceção/monitorização em tempo real. Benjamim da Silva Rodrigues, descrevendo a operação técnica de monitorização em tempo real, ensina que é possível proceder-se à "«clonagem» do *e-mail* em «trânsito», através do «desvio» para um terminal de armazenamento digital de uma cópia da mensagem posta a circular na rede pública de comunicações eletrónicas"[277].

Como visto, apesar de ser tecnicamente possível a monitorização em tempo real do correio eletrónico enquanto circula na rede, há que questionar se o regime das escutas telefónicas é o mais adequado para esse fim, tal como consagrado no artigo 189.º n.º 1 CPP.

[275] No mesmo sentido entende Benjamim da Silva Rodrigues em Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 431.
[276] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 181.
[277] Benjamim da Silva Rodrigues em Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 445.

As escutas telefónicas parecem ser o meio de obtenção de prova destinado à ingerência em tempo real nas conversações, a que o legislador estendeu à "interceção" do correio eletrónico – que pode ser "intercetado" mesmo antes de chegar ao terminal informático do destinatário, sob a forma de dados informáticos que transitam na Internet. Doutrina e jurisprudência têm entendido pacificamente que as escutas telefónicas são o meio correto para a ingerência em tempo real do correio eletrónico, enquanto circula na rede, traduzindo, pelas palavras de Costa Andrade, a "específica situação de perigo" em que se encontra devido ao controlo e possibilidade de ingerência do prestador de serviços, que possui o domínio sobre o correio eletrónico até este ser acedido pelo destinatário[278], consagrando-se para tal situação de perigo um regime com apertados trâmites de aplicação. Analisaremos *infra* se este deve ou não ser o regime para esta monitorização, aquando da análise do meio de obtenção de prova previsto no artigo 18.º da LC – a "transposição" do regime das escutas telefónicas para a recolha da prova em suporte eletrónico.

Fora do âmbito da monitorização em tempo real do correio eletrónico, a investigação criminal pode pretender imiscuir-se no seu conteúdo, pesquisando todo o correio eletrónico recebido e enviado pelo investigado – afastando-se da predita "ingerência em tempo-real", ou seja, enquanto a mensagem circula na rede. Parece que o artigo 189.º n.º 1 CPP também remete estas operações para o regime das escutas telefónicas. Ora, as escutas tratam-se de um meio de obtenção de prova consagrado para a ingerência em conversações telefónicas – necessariamente orais –, realizadas em tempo real entre os interlocutores e que exprime da forma mais direta a personalidade do interlocutor, sem existir a ponderação necessária para atenuações no que vai dito, ou mesmo para se ponderar que a conversa possa estar a ser escutada. A palavra oral é diferente da palavra escrita, daí que a primeira possua proteção constitucional específica[279], ao passo que a segunda apenas possua proteção como qualquer expressão humana – pela falta de reflexão do que é dito, bem como a confiança nos prestadores de serviços e no direito à não ingerência nas comunicações privadas. Assim, não faz sentido que as "buscas" do correio eletrónico enviado e recebido se pautem pelos trâmites de um meio de obtenção de prova com apertados requisitos de realização e validade.

[278] Como se retira de Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 164.
[279] Como analisado *infra*, capítulo I, ponto 2. a) ii) do presente trabalho.

Quando se escreve, sabe-se que se eterniza uma mensagem, seja privada ou não, existindo uma "ponderação que vai implicada na mensagem que se transmite e que se põe ao dispor de quem a recebe. Sabe-se que no momento em que se põe a correspondência escrita em circulação – seja através dos serviços postais públicos, seja através dos serviços de comunicações eletrónicas publicamente disponíveis relacionados com a *internet* – deixamos de ter controlo na mesma, podendo o(s) destinatário(s) que escolhemos, desde que não sujeito(s) a especial dever de sigilo, apresenta-lo a terceiros. Ao enviar a mensagem que pretendemos comunicar de forma escrita, aceitamos perpetuá-la"[280].

Acompanhando neste ponto Rita Castanheira Neves, defendemos que é importante a distinção dos regimes dos meios de obtenção de prova que se destinem à interceção de comunicações faladas e escritas, devido à diferente volatilidade que existe entre as duas realidades: quando se comunica com outrem através de chamadas voz, pretende-se que a palavra se extinga naquele momento e uma vez captada pelo seu destinatário, não sendo cunhado no que foi dito a intenção de perpetuação e registo. O que não acontece quando se opta por escrever alguma mensagem de correio eletrónico: confere-se perenidade pela forma escrita, acompanhada da ponderação necessária inerente a essa mesma perenidade, podendo assumir a forma de documento, físico ou virtual, sendo muitas vezes difícil eliminá-lo definitivamente, devido aos diversos *backups* que diversas aplicações e *softwares* realizam, mesmo sem comando direto (e, muitas das vezes, autorização) do utilizador. Assim, consideramos que existe a total desvirtuação do paradigma constitucional e teleológico que sustenta as escutas telefónicas, quando se estende o seu regime à ingerência em comunicações que se processam por via escrita e que se encontram armazenadas – e por isso, opostas às chamadas telefónicas que são "escutáveis".

Parece que o legislador pretende, através do artigo 189.º n.º 1 CPP, estender o acesso ao correio eletrónico que já foi recebido, lido e armazenado ao regime das escutas telefónicas, pela mão do inciso "mesmo que guardados em suporte digital". Paulo Dá Mesquita considera que esta opção "revela uma inequívoca intenção de que a cessação do ato de envio eletrónico (relativo a escrito, som e/ou imagem) não corresponda ao fim do âmbito de tutela extensiva

[280] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 173.

do regime das escutas, nomeadamente a exigência de integração num crime de catálogo e reserva judicial"[281] – o que, a seu ver e no que concordamos, gera uma diferença substancial e infundada diferença entre mensagem de correio eletrónico que é impressa e a que é guardada em suporte digital, estando a primeira sujeita ao regime geral das buscas, e a segunda – conforme o que faz parecer o artigo 189.º n.º 1 CPP (e a quem desconhecer a Lei do Cibercrime), ao regime das escutas telefónicas.

Passemos à análise dos meios de obtenção de prova relativos ao correio eletrónico consagrados na Lei do Cibercrime, de modo a tentar compreender qual é, afinal, o regime que rege a ingerência no conteúdo do correio eletrónico.

c) O artigo 17.º da Lei do Cibercrime

i. A opção legislativa

Do artigo 17.º LC[282] consta o meio de obtenção de prova relativo à "apreensão de correio eletrónico e registos de comunicações de natureza semelhante": "quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal" (sublinhado nosso).

Trata-se da consagração de solução bastante diversa da preconizada no artigo 189.º n.º 1 CPP, no que toca ao acesso ao conteúdo do correio eletrónico depois de recebido e armazenado: em primeiro lugar, trata-se da apreensão de *eventual* correio eletrónico

[281] Mesquita, Paulo Dá. Processo Penal, Prova e Sistema Judiciário. 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 91.
[282] Que, segundo Rita Castanheira Neves, se trata de uma das novidades da Lei do Cibercrime, dado que este meio de obtenção de prova não encontra paralelo na Convenção sobre a Criminalidade – conforme se retira de Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 273.

descoberto em sistemas informáticos no decurso de qualquer acesso a estes; em segundo lugar, este meio de obtenção de prova é aplicável em todas as investigações de crimes previstos na Lei n.º 109/2009 e quaisquer crimes que sejam cometidos por meio de sistema informático ou em relação ao qual seja necessário proceder à recolha de prova em suporte eletrónico (conforme o artigo 11.º n.º 1 LC); em terceiro lugar, remete para o regime da apreensão da correspondência, e não para o das escutas telefónicas[283].

Armando Dias Ramos considera que o correio eletrónico não deve ser equiparado ao correio tradicional, e por isso a ingerência no seu conteúdo não deve ser remetida para o regime da apreensão de correspondência: em primeiro lugar, pela possibilidade de filtragem de mensagens pelo servidor de correio eletrónico, sendo "usual e comummente aceite que um gestor/administrador dos sistemas informáticos de uma empresa ou de um serviço público coloque filtros no servidor de correio eletrónico tentando, desta forma, filtrar e barrar a passagem deste tipo de mensagens"[284] – entendendo o Autor que não poderia nunca esta opção ser subsumível ao artigo 194.º e 384.º CP. Em segundo lugar, o Autor faz referência à possibilidade do envio em massa de mensagens de correio eletrónico, sem qualquer intervenção humana e de maneira a disseminar vírus informáticos e programas maliciosos nos sistemas informáticos em que o correio eletrónico for acedido – situação que seria impossível de realizar através do correio eletrónico tradicional[285]. Outro aspeto apontado pelo Autor para diferenciar o correio eletrónico do correio tradicional é a "impossibilidade de determinar quando é que uma mensagem de correio eletrónico foi lida ou não, pois não existem programas informáticos forenses que determinem essa operação, existindo sempre a possibilidade de marcar uma mensagem como «não lida», mesmo após ter sido lida"[286] – ao

[283] Paulo Dá Mesquita entendia que o legislador de 2007, ao "não adaptar o acesso a comunicações escritas por via telemática ao regime da apreensão de correspondência (…) foi acompanhada pelo aparente desinteresse na ponderação de critérios distintivos dos diferentes âmbitos de proteção à luz dos respetivos parâmetros constitucionais", tendo também o legislador, em 2009, atuado com a mesma leveza, ao submeter a apreensão do correio eletrónico ao regime da apreensão de correspondência – conforme se retira de Mesquita, Paulo Dá. Processo Penal, Prova e Sistema Judiciário. 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 93.

[284] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 64.

[285] Apesar de já terem sido perpetuados ataques terroristas através do correio tradicional, através do envio de envelopes contaminados com bactérias manipuladas, de maneira a disseminar o "antraz", ataque batizado como "Amerithrax", realizado nos Estados Unidos em 2001 – como se relembra através de http://www.jn.pt/mundo/interior/eua-inquerito-sobre-cartas-com-anthrax-concluido-1499717.html, acedido e consultado a 22-08-2017.

[286] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 69.

contrário do correio eletrónico tradicional, em que após aberto o suporte físico em que o correio foi transmitido, não há volta a dar: o envelope será violado. Para além disso, o Ilustre Autor aponta a possibilidade de se criar uma multiplicidade de contas em diversos servidores de *e-mail*, pertencentes à mesma pessoa, ou mesmo a criação de contas com o mesmo nome, pertencentes a pessoas distintas, através de diferentes servidores – o que pode levar ao envio de correio eletrónico para pessoa distinta da pretendida, o que é difícil de acontecer no correio tradicional, apesar de possível, uma vez que a morada física da pessoa é um dado facilmente comprovável[287]. No entender deste Autor, este é mais um ponto que comprova a sua tese de não equiparação do correio eletrónico ao correio tradicional: considera que o correio eletrónico deve ser tratado com um mero ficheiro informático[288].

O legislador de 2009 optou por consagrar, quando se trate da descoberta de correio eletrónico em pesquisas efetuadas a sistemas informáticos, que "o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal" – artigo 17.º LC. No entanto, ao fazê-lo não procedeu à diferenciação que se impunha: este meio de obtenção de prova dirige-se à apreensão *de que* mensagens de correio eletrónico? Às que ainda não foram abertas e lidas pelo destinatário, às mensagens que já foram abertas e o seu conteúdo conhecido e armazenado, ou a ambas? Nem respondeu à questão de saber qual é o meio de obtenção próprio para a pesquisa específica de correio eletrónico nos sistemas informáticos – pois não se esqueça que o artigo 17.º LC apenas se dirige à apreensão do correio eletrónico quando este for encontrado no decurso de pesquisas a sistemas informáticos. Impõe-se também a questão de saber se é possível e qual o meio para a "interceção" do correio eletrónico "em tempo real" – enquanto transita na rede o regime – ao que não é aplicável o meio de obtenção de prova consagrado no artigo 17.º LC, levantando-se a questão da aplicabilidade do regime previsto no artigo 18.º LC.

[287] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico*. 2ª. Chiado Editora, 2017. Página 75.
[288] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 175.

ii. A tutela do correio eletrónico

Paulo Dá Mesquita considera que reduto da "apreensão de correio eletrónico" é a apreensão de correio eletrónico que ainda não foi aberto e lido pelo destinatário[289], pois considera essencial não esquecer que "a tutela do artigo 179.º n.º 1 CPP (e do artigo 34.º da Constituição) se reporta à comunicação em curso e não ao conteúdo da comunicação já acedida por parte do destinatário (que decide guardá-la)"[290].

Em sentido contrário entende João Conde Correia: "numa perspetiva literal, não tendo ele [o legislador] estabelecido qualquer distinção legal, também o intérprete não deverá separar, beneficiando o correio aberto e lido do regime previsto para todo o restante"[291]. De facto, parece que a intenção do legislador, ao não distinguir entre os diferentes tipos de correio eletrónico – leia-se, já recebidos, mas lidos ou não – remetendo-os para o mesmo regime de "apreensão", quis que fosse dado o mesmo valor à correspondência eletrónica já aberta e lida, que contém registos do que outrora fora comunicação, e ao correio eletrónico cujo conteúdo ainda não foi conhecido pelo destinatário.

Entende Rita Castanheira Neves que "a Lei do Cibercrime consagra uma distinção para o *e-mail* armazenado, que nem equipara à proteção da interceção do *e-mail* enquanto comunicação, nem à (falta de) proteção de normais escritos. De facto, reconhece esta lei um *plus* de proteção a arquivos que já foram comunicação, em nome da salvaguarda da privacidade da autodeterminação informacional, remetendo para o regime de correspondência"[292]. O de facto, e salvo o devido respeito por melhor opinião, carece de sentido, pois tratam-se de documentos semelhantes a quaisquer documentos físicos (apesar de diferentes a vários níveis, bem como aos diferentes vestígios que possuem)[293], cuja recolha

[289] Mesquita, Paulo Dá. Processo Penal, Prova e Sistema Judiciário. 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 118.
[290] Mesquita, Paulo Dá. Processo Penal, Prova e Sistema Judiciário. 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 117.
[291] Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 40.
[292] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 276.
[293] Os documentos físicos podem conter vestígios biológicos que podem ser recolhidos, ao passo que os documentos informáticos, através da realização de perícias, contêm o diversas informações, que podem ir desde a data de criação do ficheiro ao local da criação.

para o processo criminal possui requisitos mais apertados do que a recolha de documentos físicos, o que onera injustificadamente a investigação criminal.

O regime consagrado para o correio tradicional, para o qual remete o artigo 17.º LC, prevê a diferenciação do correio já aberto e lido do que ainda não o foi, em homenagem à tutela da privacidade e da correspondência escrita, bem como do seu sigilo: se o correio já tiver sido aberto, aplica-se o regime geral das apreensões – artigo 178.º CPP, sendo as mesmas autorizadas ou ordenadas por despacho da autoridade judiciária, podendo ainda ser validadas quando realizadas pelos Órgãos de Polícia Criminal em determinadas situações (artigo 178.º n.º 4 CPP); ao passo que se o correio não tiver sido lido, aplica-se a apreensão da correspondência (dita "tradicional") – artigo 179.º CPP, sendo necessária ordem ou autorização do juiz, nos casos em que a "correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa", quando "está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos", e "a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova". A *ratio* da distinção é facilmente alcançável: nos casos em que o destinatário ainda não teve acesso ao conteúdo da correspondência que lhe foi dirigida, a ingerência da investigação criminal será mais gravosa e os direitos fundamentais do destinatário serão mais comprimidos em nome daquela, o que sempre será atenuado nos casos em que o destinatário já teve conhecimento do conteúdo da correspondência.

Consideramos que a diferenciação de regimes entre o correio eletrónico aberto e lido e o que ainda não o foi, tal como feita no correio tradicional, cuja essência é a mesma sob o ponto de vista do seu conteúdo[294], era assim necessária também em relação ao correio eletrónico sob o ponto de vista teleológico, tratando-se de uma intromissão altamente mais violadora quando se trata da ingerência em correspondência cujo conteúdo o destinatário ainda não tomou conhecimento. No entanto, no que ao correio eletrónico diz respeito, não se esquece as dificuldades que o acompanham, derivadas das múltiplas possibilidades técnicas que lhe assistem: marcação de *e-mails* já lidos como se não o fossem, mensagens enviadas em massa, não solicitadas e sem qualquer intervenção humana, podendo conter publicidade

[294] Também Pedro Verdelho o entende: "De facto, na sua essência em nada divergem de uma carta remetida pelo correio físico, dito tradicional" – como se retira de Verdelho, Pedro. "A obtenção de prova no ambiente digital." *Revista do Ministério Público*, Julho-Setembro de 2004, ano 25: 117-136. Página 123.

ou vírus informáticos (as mensagens *SPAM*[295]), e a multiplicidade de contas que cada pessoa pode ter, tornando o correio eletrónico uma opção perfeita no mundo do anonimato informático. No entanto, estas dificuldades não obstariam à consagração de regimes diversos consoante a leitura ou não do correio eletrónico, uma vez que na sua essência, apesar de todas as possibilidades técnicas que assistem ao correio eletrónico, o conteúdo deste é semelhante ao do correio tradicional, para além de que é possível a realização de perícias informáticas de modo a averiguar a possível leitura e desmarcação como tal.

Parece que a intenção do legislador foi mesmo a de não proceder a esta distinção, tanto que expressamente consagrou a apreensão de "correio eletrónico *e registos de comunicações de natureza semelhante*" (itálico nosso). Quanto a este inciso, parece que o legislador, tal como havia feito no artigo 189.º n.º 1 CPP, pretende consagrar um acréscimo de proteção em relação aos arquivos informáticos que contenham correio eletrónico ou registos de comunicação de natureza semelhante[296], remetendo-os para o mesmo regime de apreensão de correspondência: quando se tratam de meros ficheiros informáticos respeitantes ao que foi, outrora, comunicações semelhantes ao *e-mail*. Intenção essa que não compreendemos nem concordamos, uma vez que os registos que contêm o que foi, outrora, comunicação, deixam de ser comunicação por natureza, não reclamando a mesma proteção que a esta reclama – por se tratarem de arquivos daquelas, que devem ter o mesmo valor de quaisquer documentos físicos. A única diferença em relação a estes é o seu formato – digital –, não reclamando proteção acrescida para o acesso da investigação ao conteúdo dos registos, devendo poder ser facilmente acessível através de pesquisas informáticas, consagradas no artigo 15.º da LC[297] (tais como as buscas e apreensões tradicionais de documentos físicos, consagradas no Código de Processo Penal).

Perante as dificuldades que se avultam, uma solução possível seria diferenciar as mensagens de correio eletrónico que fossem assinadas digitalmente das que não o são, podendo a assinatura conferir mais segurança quanto ao remetente do *e-mail*, e mais

[295] Cuja sigla significa "*Sending and Posting Advertisement in Mass*".
[296] Que averiguaremos *infra* se se considera ser o caso dos *SMS* e *MMS*, bem como as conversações mantidas através de mensagens instantâneas pela Internet.
[297] Artigo 15.º n.º 1 LC: "Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência".

facilidade na sua identificação – de modo a afastar algumas das críticas enunciadas. Por assinatura digital designa-se "qualquer método de assinatura de documento eletrónico que permita identificar o seu autor, desempenhando esta funções similares à assinatura manual em documento escrito"[298] – assinatura regulada pelo Decreto-Lei 290-D/99. Assim, conforme o artigo 6.º n.º 3 deste Decreto-Lei: "A comunicação do documento eletrónico, assinado de acordo com os requisitos do presente diploma, por meio de telecomunicações que assegure a efetiva receção equivale à remessa por via postal registada e, se a receção for comprovada por mensagem de confirmação dirigida ao remetente pelo destinatário com assinatura digital e recebida pelo remetente, equivale à remessa por via postal registada com aviso de receção" – parece que também aqui se remete para o correio tradicional. No entanto, mesmo que o *e-mail* seja assinado digitalmente não confere ao correio eletrónico as mesmas características do correio tradicional, podendo ser na mesma marcado como não lido após o ter sido, nem conferir sequer a essência de correio eletrónico – qualquer documento pode ser assinado sem que seja correspondência, podendo tratar-se de um mero documento a que se quis conferir autenticidade reforçada com a assinatura digital.

Outra solução poderia passar pela desconsideração da possibilidade de marcação dos *e-mails* como não lidos após o terem sido, e realizar a distinção de regimes a partir dessa característica: terem sido lidos ou não, aplicando-se um regime mais protecionista em relação aos que ainda não o foram. Poder-se-ia realizar perícias informáticas aos *e-mails* não lidos, a fim de averiguar da sua possível leitura e marcação como não o sendo: mas reconhece-se que estes procedimentos iriam onerar a investigação criminal, sendo necessários diversos procedimentos técnicos para averiguação de qual o regime aplicar a cada *e-mail* constante da caixa de correio eletrónico, que podem ascender a números incalculáveis, o que retiraria conteúdo útil à medida.

Parece que a solução que deveria ser dada ao correio eletrónico já lido e o seu conteúdo conhecido é de fácil resolução, devendo ser considerado como um mero ficheiro informático: pelo facto de o destinatário já ter conhecimento do conteúdo do *e-mail* não deve ser necessário submetê-lo aos trâmites do meio de obtenção de prova do artigo 17.º LC (que

[298] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 108.

remete para a apreensão de correspondência), e sim à apreensão de dados informáticos plasmada no artigo 16.º LC[299] – após a realização de pesquisas informáticas, consagradas no artigo 15.º LC.

Afinal, tratam-se de registos de comunicações, em tudo semelhantes a qualquer documento informático armazenado em suporte eletrónico, constituindo registos que já foram analisados e tratados pelo destinatário (nem que seja abertura do e-mail ou arquivo no sistema informático), o que reclama um nível de proteção menor em relação ao correio eletrónico que não foi lido, sendo suficiente a intervenção do magistrado do Ministério Público para que os registos do correio eletrónico já lido pudessem ser validamente apreendidos[300], prescindindo-se da ordem ou autorização do juiz para a válida apreensão.

Tal como Conde Correia, consideramos algo caricato o facto de, "por estranho que pareça, o Ministério Público pode apreender uma carta guardada num cofre, mas não um *email* guardado num computador"[301]. Resta assim a solução de eliminar o inciso "e registos de comunicações de natureza semelhante" do artigo 17.º LC, ao que se deveria aplicar o regime das pesquisas informáticas e a posterior apreensão dos dados recolhidos (aplicando-se os artigos 15.º e 16.º LC, respetivamente).

Quanto ao correio eletrónico que ainda não foi aberto e o seu conteúdo conhecido, face a todas as características que o afastam do correio tradicional, tais como a possibilidade de marcar uma mensagem como não lida mesmo quando o foi, a de cada utilizador possuir uma multiplicidade de contas de *e-mail* o que potencia o anonimato no mundo informático e ainda o envio por engano de correio eletrónico para pessoas distintas das pretendidas, faz com que Armando Dias Ramos entenda que também este correio eletrónico deva ser tratado como qualquer ficheiro informático[302]. No entanto, pensamos que esta solução desconsidera a afirmação do correio eletrónico enquanto forma de comunicação assumidamente séria entre

[299]Artigo 16.º n.º 1 LC: "Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos".

[300] No mesmo sentido se exprime em Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 41.

[301] Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 41.

[301] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico*. 2ª. Chiado Editora, 2017. Página 175.

os indivíduos, através da qual se transmitem muitas informações pessoais e confidenciais e até se realizam contratos, apesar da vertente publicitária e muitas vezes não séria que assume – mas o todo não deve ser catalogado pela parte, sendo de dar tanta importância ao correio eletrónico como a que é dada ao correio tradicional, não devendo ser estabelecido um regime de ingerência no correio eletrónico que não tome em conta os direitos fundamentais dos indivíduos, tratando-a como uma forma "menor" de ingerência ao nível da privacidade.

Parece-nos que neste ponto não andou mal o legislador quando remeteu para o regime da apreensão do correio tradicional o correio eletrónico ainda não aberto, descoberto no decurso de acessos legítimos aos sistemas informáticos do investigado, pois os direitos fundamentais e valores em causa são os mesmos: proteção da confidencialidade da correspondência (não sendo necessário distinguir entre tradicional e eletrónica pois reconduz-nos à mesma realidade, separada pela diferença de meios técnicos) e do sigilo dos prestadores de serviços, bem como a privacidade dos indivíduos. Quanto ao correio eletrónico que já foi aberto e lido pelo destinatário, pensamos que o legislador deveria ter enquadrado na categoria de dados informáticos armazenados, também acessíveis pela investigação criminal, mas que já não constituem comunicação.

No entanto, parece que o elemento literal do artigo 17.º LC afasta a possibilidade de qualquer entendimento que faça a diferenciação entre o correio eletrónico já aberto e lido e o que ainda não o foi, pois *ubi lex non distinguit nea nos distinguere debemos*, acrescendo ainda as dificuldades introduzidas pela extensão da aplicação do regime de apreensão do correio eletrónico aos "registos de comunicações de natureza semelhante" daquele. Assim, mais uma vez "o legislador não foi muito claro, deixando espaço suficiente para a polémica desnecessária e inútil"[303], parecendo que a sua intenção foi remeter *todo* o correio eletrónico descoberto no acesso a sistemas informáticos, tenha sido lido ou não, para o mesmo regime de apreensão – a que destina a apreensão de correspondência, o que demonstra a incongruência da solução.

[303] Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 40.

iii. Trâmites processuais

A apreensão de correio eletrónico prevista no artigo 17.º LC é um meio de obtenção de prova que se destina à investigação de um amplo leque de crimes, abrangendo todos os constantes do artigo 11.º LC: previstos na Lei do Cibercrime[304], os "cometidos por meio de um sistema informático"; ou "em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico": ou seja, todos os tipos de crimes.

Este meio de obtenção de prova destina-se à apreensão de correio eletrónico encontrado no "decurso de pesquisas informáticas ou outro acesso legítimo a sistema informático". Quanto às pesquisas informáticas, encontram-se previstas no artigo 15.º LC, sendo realizadas "quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência" (número 1). Ou seja, a pesquisa de dados informáticos pode ser realizada na investigação de um grande leque de crimes, que se pode traduzir necessidade de pesquisas a telemóveis, cartões de memória, cartões *SIM*, computadores, *pen drives* ou discos rígidos – quaisquer aparelhos informáticos.

Quanto ao inciso "outro acesso legítimo a sistema informático" constante do artigo 17.º LC e que permite a descoberta do correio eletrónico, considera Paulo Dá Mesquita que pode ser o acesso ao sistema informático previsto no artigo 18.º LC, através da "interceção de comunicações"[305]. Consideramos que se trata de um bom entendimento, uma vez que a interceção de comunicações prevista no artigo 18.º LC se trata de um meio de obtenção de prova de que se pode lançar mão autonomamente, para um determinado leque de crimes e respeitando determinados trâmites processuais, e que se destina à ingerência ou monitorização do correio eletrónico enquanto circula na rede. Assim, após o término do trânsito do correio eletrónico, quando chega ao terminal do destino, pode ter-se conhecimento

[304] Ou seja, os crimes de falsidade informática, consagrado no artigo 3.º; de dano relativo a programas ou outros dados informáticos, artigo 4.º; de sabotagem informática, artigo 5.º; de acesso ilegítimo, artigo 6.º; de interceção ilegítima, artigo 7.º; de reprodução ilegítima de programa protegido, artigo 8.º e de perda de bens, artigo 10.º.
[305] Conforme se retira de Mesquita, Paulo Dá. Processo Penal, Prova e Sistema Judiciário. 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 120.

do correio eletrónico nele armazenado, tenha sido ou não acedido pelo destinatário. Por isso, tendo a investigação conhecimento da existência de correio eletrónico e *registos* de comunicações semelhantes, deve ser aplicável o artigo 17.º LC (que, como visto, parece ser aplicável ao correio eletrónico já lido e o que ainda não o foi, apesar de considerarmos que apenas deve ser aplicável ao correio eletrónico que não foi lido).

Quanto aos trâmites deste meio de obtenção de prova, Pedro Verdelho considera que a Lei do Cibercrime não exige despacho judicial para a apreensão do correio eletrónico, apenas sendo necessária a "existência de uma forma legítima de acesso ao meio informático em que estavam armazenadas"[306] – não se esqueça que se trata da apreensão de correio eletrónico encontrado no decurso de pesquisas informáticas ou acesso a aparelhos informáticos, o que faz com que, à partida, não se conheça da existência de correio eletrónico neles armazenado. Parece ser a única interpretação correta da solução adotada pela Lei do Cibercrime, que vai de encontro às exigências dos casos concretos. Antes da consagração desta solução, já vários Autores apontavam a existência de prévio despacho judicial para a apreensão de correio eletrónico como algo que traria grandes dificuldades de exequibilidade, uma vez que "se é verdade que é frequente em buscas, domiciliárias ou não, proceder à apreensão de computadores ou outros equipamentos, quando se desconhecia, no momento da autorização da diligência, o que poderia ser encontrado nos espaços visados, não se mostra possível obter, para grande parte dos casos, autorização judicial específica para a «recolha» de mensagens, rececionadas ou remetidas, nos ditos equipamentos compatíveis com o n.º 1 do artigo 189.º CPP, nem ainda se mostra possível ou operacional observar o procedimento do artigo 188.º CPP (…)"[307].

Face às dificuldades da vida prática, que guiam e enformam qualquer investigação e que por isso devem ser atendidas pelo legislador, é fácil concluir que não seria viável que se exigisse autorização e despacho judicial prévio à apreensão de correio eletrónico no decurso

[306] Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Iuridica*, Outubro-Dezembro de 2009, n.º 320. Página 743.
[307] Teixeira, Carlos Adérito. "Escutas telefónicas: a mudança de paradigma e os velhos e os novos problemas." *Revista do CEJ*, 1º semestre de 2008, nº 9: 243-295. Página 282.

de pesquisas ou acessos a sistemas informáticos, que sempre seriam eventuais e a sua existência desconhecida *a priori*[308].

Pedro Verdelho entende que não é necessário que o juiz seja o primeiro a ter conhecimento do conteúdo dos *e-mails*, o que é necessário na apreensão de correio físico, parecendo que "a letra da lei aponta antes para a possibilidade de quem procede à pesquisa encaminhar para o juiz mensagens concretas, com relevância para o caso concreto, que aquele depois apreenderá ou não"[309]. Até porque as mensagens de correio eletrónico serão descobertas no preciso decurso das pesquisas ou acessos aos sistemas informáticos, não sendo tecnicamente possível impedir o conhecimento do conteúdo dos *e-mails* ou ficheiros que se encontrar, reservando-o para o juiz. Assim, a entidade que realizar as buscas terá a tarefa de, encontrando correio eletrónico, selecionar os que se afiguram de maior importância para a investigação criminal, apresentando-o ao juiz para que ordene ou autorize a junção destes ao processo – seria muito difícil qualquer juiz aferir da possibilidade de autorizar ou não a junção de correio eletrónico sem existir a pré-seleção dos *e-mails* com relevância pela entidade investigatória.

O regime consagrado no artigo 17.º LC parece apontar no sentido de que, tal como na apreensão de correio físico, na apreensão de correio eletrónico se permite a apreensão provisória e cautelar das mensagens de correio eletrónico, nos termos do artigo 252.º do CPP[310]: uma vez que na apreensão de correio eletrónico no âmbito deste meio de obtenção de prova a intervenção judicial é exigida em momento posterior – logicamente, após se ter conhecimento da existência de correio eletrónico. Assim, pode apreender-se correio eletrónico de forma cautelar e sem prévio despacho judicial, sendo este necessário num

[308] No mesmo sentido entende Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Iuridica*, Outubro-Dezembro de 2009, n.º 320. Página 744.
[309] Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Iuridica*, Outubro-Dezembro de 2009, n.º 320. Página 744.
[310] Que consagra que: "1: Nos casos em que deva proceder-se à apreensão de correspondência, os órgãos de polícia criminal transmitem-na intacta ao juiz que tiver autorizado ou ordenado a diligência. 2: Tratando-se de encomendas ou valores fechados suscetíveis de serem apreendidos, sempre que tiverem fundadas razões para crer que eles podem conter informações úteis à investigação de um crime ou conduzir à sua descoberta, e que podem perder-se em caso de demora, os órgãos de polícia criminal informam do facto, pelo meio mais rápido, o juiz, o qual pode autorizar a sua abertura imediata. 3: Verificadas as razões referidas no número anterior, os órgãos de polícia criminal podem ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações. Se, no prazo de quarenta e oito horas, a ordem não for convalidada por despacho fundamentado do juiz, a correspondência é remetida ao destinatário".

segundo momento, para que se possa utilizar tais mensagens como meio de prova num processo criminal.

Entendemos, no seguimento dos ensinamentos de Pedro Verdelho, que a Lei do Cibercrime apenas reproduziu o requisito constante na alínea c) do número 1 do artigo 179.º CPP, referente ao regime das apreensões de correspondência: a "diligência se revelará de grande interesse para a descoberta da verdade ou para a prova", parecendo que o legislador apenas pretendeu que fosse este o único requisito do regime de apreensão de correspondência o único aplicável a este meio de obtenção de prova[311]. Assim, "quando forem encontradas mensagens de correio eletrónico ou registos de comunicações de natureza semelhante em sistemas informáticos, a junção ou não destas mensagens será determinada por um juiz, se tais mensagens se afigurarem ser de grande interesse para a descoberta da verdade ou para a prova"[312].

Em sentido contrário entendeu o Tribunal da Relação de Lisboa, a 11 de janeiro de 2011[313], que considerou que " a Lei do Cibercrime (Lei nº109/09, de 15Set.), ao remeter no seu art.17, quanto à apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, para o regime geral previsto no Código de Processo Penal, determina a aplicação deste regime na sua totalidade, sem redução do seu âmbito" – sendo por isso necessária a verificação dos requisitos plasmados no artigo 179.º do CPP.

No mesmo sentido entende Rita Castanheira Neves, entendendo que o artigo 17.º LC remete para quatro aspetos do regime do artigo 179.º CPP: "à referência à nulidade no caso de não respeito pelos requisitos estabelecidos (n.º 1 e 2 do artigo 179.º CPP); ao facto de ter que estar em causa correio eletrónico e registos de comunicações de natureza semelhante enviado ou recebido pelo suspeito, mesmo que de/a partir de endereço eletrónico de pessoa diversa (alínea a) do n.º 1 do mesmo artigo 179.º); à proibição de apreensão do correio eletrónico e registos de comunicação de natureza semelhante trocado entre o arguido e

[311] No mesmo sentido entende Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Iuridica*, Outubro-Dezembro de 2009, n.º 320. Página 746.
[312] Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Iuridica*, Outubro-Dezembro de 2009, n.º 320. Página 745.
[313] Processo n.º 5412/08.9TDLSB-A.L1-5, relator: Ricardo Cardoso. Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e5ed1936deb44eb180257824004ab09d?OpenDocument. Acedido em 10 de junho de 2017.

defensor, salvo se o juiz tiver fundadas razões para crer que aquele correio eletrónico ou aqueles registos constituem objeto ou elemento do crime (n.º 2 do artigo 179.º); e finalmente ao facto de ter que ser o juiz que tiver autorizado ou ordenado a diligência a primeira pessoa a tomar conhecimento do conteúdo do correio eletrónico e demais registos de comunicação apreendido, mandando-o juntar ao processo se o considerar relevante"[314].

Armando Dias Ramos descreve o procedimento adotado na recolha do correio eletrónico: "A maioria das vezes o juiz ordena que a Polícia Judiciária proceda ao desencapsulamento das mensagens e indique quais as que considera relevantes para juntar aos autos, efetuado o seu respetivo *print*. Outras vezes, esta diligência requer que um perito de informática, por norma da Polícia Judiciária, se desloque ao gabinete do Magistrado Judicial para o auxiliar nessa tarefa, sendo que aqui, para além do juiz, mais alguém (o perito, ainda que este se encontre subordinado ao dever de sigilo) toma conhecimento imediato das mensagens de correio eletrónico"[315]. Este Autor invoca neste ponto a dificuldade do Juiz de ter contacto com todas as mensagens de correio eletrónico a fim de decidir quais devem ser juntas ao processo, uma vez que podem ser milhares – ao contrário do correio eletrónico tradicional, em que não é usual existir muita correspondência apreendida. Para além desta dificuldade, Rita Castanheira Neves aponta a dificuldade de "restituição" do correio eletrónico visado pela apreensão, "pois não se pode restituir correspondência virtual que foi gravada para ser levada ao juiz, mas que, no fundo, nunca saiu do computador/espaço virtual onde se encontrava"[316].

d) O artigo 18.º Lei do Cibercrime

O artigo 18.º da LC consagra a "interceção de comunicações" eletrónicas. Paulo Dá Mesquita, socorrendo-se das definições apresentadas pela Lei do Cibercrime (e importadas sem grandes adaptações dos normativos internacionais), entende que por "interceção" se

[314] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 274.
[315] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 72.
[316] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 185.

entende "o ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros" – artigo 2.º e) LC.

A interceção de comunicações pode "destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego" [317] – artigo 18.º n.º 3 LC, sendo que a "interceção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, 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, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público" (número 2 do mesmo artigo). A interceção de comunicações em tempo real apenas pode ser utilizada relativamente à investigação de crimes previstos na Lei do Cibercrime, e ainda aos "cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal".

Impõe-se a questão de saber se este meio de obtenção de prova se destina à "interceção de correio eletrónico em tempo real", e em que momento essa interceção pode ser realizada: trata-se da interceção em tempo real do correio eletrónico enquanto circula na rede, tal como o regulado no artigo 189.º n.º 1 CPP?

Já em 2008 Benjamim da Silva Rodrigues entendia que é importante delimitar o que seja a interceção do correio eletrónico e as diferentes fases em que pode ser feita: "por um lado, temos aquelas situações em que o *e-mail* enviado já foi recebido mas ainda não foi consultado pelo seu titular e, por outro lado, temos os casos em que o *e-mail* é monitorizado

[317] Quanto à distinção entre interceção em tempo real de dados de tráfego e de conteúdo, ensina Benjamim da Silva Rodrigues, socorrendo-se do estabelecido na Convenção sobre o Cibercrime, nos seus artigos 20.º e 21.º, que "existe um certo consenso acerca da distinção a efetuar, ao nível dos requisitos jurídicos, para efetuar a interceção em tempo real de dados relativos ao conteúdo e a recolha em tempo real de dados de tráfego. Deste modo, a recolha de dados de conteúdo estaria rodeada de restrições mais importantes do que os dados de tráfego, no que tange à sua recolha e acesso. Procedeu-se ao uso de uma terminologia diferenciada, consoante se esteja perante uma recolha de dados de tráfego, caso em que se falará em «recolha em tempo real», e a recolha de dados de conteúdo, situação em que se falará em «interceção em tempo real»" – como se retira de Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 348.

em tempo real, ou seja, quando se encontra «a caminho do seu destino»"[318], havendo, por último, "aquelas situações em que o *e-mail* se encontra armazenado no computador após ter sido visionado pelo seu destinatário" – considerando o Autor que quando monitorizado em tempo real, "a caminho do seu destino", deve ser aplicado o regime das escutas telefónicas, entendimento que o legislador pareceu acolher no artigo 18.º LC[319]. Este Autor considera que, "à semelhança do que acontece com as comunicações telefónicas, a monitorização de dados de conteúdo ou o próprio conteúdo das comunicações eletrónicas só poderá ser levada a cabo com a monitorização das comunicações, em tempo real, com o auxílio de uma operação técnica que permita recolher, gravar ou registar o conteúdo do fluxo informacional e comunicacional digital sem, no entanto, sublinhe-se, o entravar ou obstar a que a relação intercomunicativa se estabeleça com sucesso entre o emissor e o recetor"[320].

Por sua vez, em 2009, também Costa Andrade o entendia: "depois de recebido, lido e guardado no computador do destinatário, um *e-mail* deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito"[321]. Assim, pois deixaria de estar no âmbito da "específica situação de perigo" derivada do controlo que o *provider* continua a exercer sobre o correio eletrónico – enquanto não abrisse a mensagem, e esta permanecesse sob o domínio do prestador de serviços, sendo necessário um ato de "chamada" do correio eletrónico pelo destinatário para o acesso ao mesmo. Enquanto a mensagem permanecesse "em trânsito" e sob o domínio do prestador de serviços, o Autor entende que a proteção deveria ser mais forte, em nome da tutela do sigilo das comunicações, a que o Ilustre Autor considera ser aplicável o regime das escutas telefónicas[322].

---

[318] Rodrigues, Benjamim Silva. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008. Página 431.

[319] O mesmo entende o Autor referido: "Depois, ciente ou «escutando» algumas das nossas críticas, o legislador veio «emendar a mão», e, cautelosamente, veio referir que, em tudo o que não for contrariado pelo artigo 18.º da LCiber 2009, à interpretação e registo de transmissão de dados informáticos é aplicável o regime da interceção e gravação de conversações ou comunicações telefónicas, constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal" – como se retira de Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 533.

[320] Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 390.

[321] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 159.

[322] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 164.

Parece que é solução doutrinalmente pacífica a de consagrar um regime semelhante ao das escutas telefónicas à ingerência em tempo real no correio eletrónico – ou seja, quando deambula na rede, desde o seu envio até à sua receção e leitura, tendo o legislador acolhido a posição maioritária no artigo 18.º LC e consagrando essa mesma solução.

Face ao exposto quanto à monitorização em tempo real do correio eletrónico enquanto circula do terminal do remetente ao do destinatário, e das considerações tecidas em relação ao artigo 17.º LC, consideramos que o artigo 18.º LC pode ser utilizado para a pesquisa em tempo real do correio eletrónico até chegar ao destinatário, sendo que, a partir desse momento, tendo-se conhecimento da existência de correio eletrónico, deve lançar-se mão do artigo 17.º LC e respeitar-se os seus trâmites para a sua recolha e utilização em processo penal. Pois que, como vimos, o legislador remete para o artigo 17.º LC a apreensão de *todo* o correio eletrónico descoberto através de pesquisas informáticas ou outros acessos aos sistemas – em que se enquadra o artigo 18.º LC. Com tal conclusão, deixa de fazer sentido a parte do artigo 189.º n.º 1 CPP que se refira ao correio eletrónico, dado existir um regime específico em lei avulsa, e que é, aliás, posterior à última revisão daquele artigo.

Quanto à ingerência nas comunicações eletrónicas, Paulo Dá Mesquita entende que o legislador poderia ter consagrado outras soluções, de modo a dissipar algumas das dúvidas que ainda hoje subsistem: "poderia o legislador português ter decidido traçar uma destrinça entre a intromissão em comunicações cujas transmissões já foram processadas pelos fornecedores de serviços e comunicações que ainda não foram transmitidas pelos fornecedores de serviços (aplicando-se o artigo 17.º às primeiras e o artigo 18.º às segundas)"[323]. "Alternativamente, pode aventar-se uma outra base distintiva a partir da tutela da confiança na prestação de serviços de telecomunicações, em que se interpretaria de forma restritiva o artigo 17.º, no sentido de se vincular a intervenção nos sistemas informáticos sem colaboração ou recurso aos meios dos fornecedores de serviços, reduzindo, consequentemente, a referência a «outro acesso legítimo a sistema informático» sem ser através dos meios próprios do fornecedor de serviço"[324].

[323] Mesquita, Paulo Dá. Processo Penal, Prova e Sistema Judiciário. 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 121.
[324] Mesquita, Paulo Dá. Processo Penal, Prova e Sistema Judiciário. 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 121.

Pedro Dias Venâncio considera que "as comunicações eletrónicas não exigem um tratamento processual distinto do consagrado para as demais comunicações, mormente no que concerne à salvaguarda do direito fundamental à inviolabilidade do domicílio e da correspondência (artigo 34.º CRP). Naturalmente que neste caso falamos da interceção de mensagens de correio eletrónico em tempo real, ou seja, no seu trajeto do computador do emissor para o computador do recetor através da rede de servidores"[325]. E acrescentamos que o mesmo deve valer para a fase posterior: depois de lidos e armazenados, deve ter o mesmo tratamento que é dado ao correio tradicional já lido e arquivado em suporte de papel – sendo necessária a diferenciação de regimes apenas no aspeto técnico das buscas e apreensões, dado que se trata de ficheiros informáticos e não físicos, mas que na sua essência correspondem ao mesmo reduto.

e) Os ficheiros anexos ao correio eletrónico

Sendo o correio eletrónico uma realidade bastante próxima do correio tradicional ao nível do *conteúdo* que é possível transmitir, a nível técnico não se pode afirmar o mesmo, possuindo o correio eletrónico uma multiplicidade de ferramentas que lhe permitem levar anexos quaisquer tipos de elementos (ficheiros, sons, imagens, e até vírus informáticos). Impõe-se, assim, a questão de saber se o regime de ingerência no correio eletrónico se estende também a estes elementos anexos ao correio eletrónico[326].

Na hipótese de o destinatário do correio eletrónico conter como anexo determinado ficheiro copiar ou armazenar esse ficheiro em qualquer sistema informático ou mesmo ou setor do disco do seu computador por exemplo, considera Armando Dias Ramos que o "juiz vai considerar que este anexo, gravado numa parte do disco ou numa partição amovível, não passa de um ficheiro, ainda que o suspeito da busca alegue que o tinha recebido por correio

[325] Venâncio, Pedro Dias. *Lei do Cibercrime anotada e comentada.* 1ª. Coimbra Editora, 2011. Página 119.
[326] A mesma questão é enunciada por Armando Dias Ramos: "Um indivíduo recebe um e-mail, no qual se encontra anexado um ficheiro. Sem ler este e-mail e o seu respetivo anexo, o referido indivíduo efetua uma cópia ou procede à gravação do anexo para o disco do seu computador ou outra qualquer partição amovível e apaga a mensagem de correio eletrónico que recebera. No caso de o indivíduo vir a ser alvo de busca e apreensão, será este ficheiro considerado ou não como correspondência enviada através de correio eletrónico?" – como se retira de Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 70 e 71.

eletrónico, que ainda não o tinha lido e que deverá, por isso, ter o mesmo tratamento que é dado, por força da equiparação legal vigente, à correspondência recebida e ainda fechada"[327].

Apesar de os ficheiros anexos ao correio eletrónico poderem ser enquadrados na categoria de "registos de comunicações de natureza semelhante" previstos no artigo 17.º LC, parece que se forem armazenados em qualquer parte suporte eletrónico, fora do constante da caixa do correio eletrónico ou de enquadramento em que seja evidente que aquele anexo é referente a determinado *e-mail*, não nos parece que deva ser considerado como "registos de comunicações de natureza semelhante", tanto que pode não dizer respeito a qualquer comunicação e ser um mero ficheiro de som ou imagem por exemplo. Assim, se não existir a ligação ao *e-mail* verificável pela entidade investigatória, deve ser tratado como um ficheiro eletrónico comum. Ao que acresce o facto de, mesmo que fosse considerado "registo de comunicação de natureza semelhante" e aplicado o regime da apreensão previsto no artigo 17.º LC, seria realizar diferenças injustificáveis entre ficheiros constantes nos sistemas informáticos – uns seriam apreendidos através do meio consagrado no artigo 16.º LC, tendo a natureza de ficheiros informáticos, outros apreendidos enquanto registos de correio eletrónico ou de comunicações de natureza semelhante, seguindo os trâmites do artigo 17.º LC.

Para concluir, entendemos que ao anexo do correio eletrónico deve ser estendido o seu regime de apreensão, nos casos em que seja integrante da mensagem, ao passo que nos casos em que for autonomizado da mesma passa a ser tratada como qualquer ficheiro informático, não havendo "qualquer razão para ser tratado como mensagem"[328].

4. As SMS (Short Message Service) e MMS (Multimedia Messaging Service)

As *SMS*, cuja sigla significa *Short Message Service*, e as *MMS*, *Multimedia Messaging Service*, afirmaram-se na vida dos cidadãos através do desenvolvimento dos

[327] Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 70.
[328] Cabral, José António Henriques dos Santos, António Pires Henriques da Graça, António Henriques Gaspar, Eduardo Maia Costa, António Jorge de Oliveira Mendes, e António Pereira Madeira. *Código de Processo Penal Comentado.* Almedina , 2014. Página 838.

telefones móveis, permitindo a troca de mensagens de texto curtas (até 160 caracteres, as SMS) e as mensagens de multimédia (com capacidade para suportar mais caracteres e elementos audiovisuais). Com a sua utilização massiva a nível mundial, mesmo após a relativa perda de importância com o surgimento de aplicações informáticas que permitem o estabelecimento de conversações através da Internet, o conteúdo das *SMS* e *MMS* recebidas e enviadas possuem bastante relevância para a investigação criminal, sendo importante definir quais os meios de obtenção de prova que se dirigem à ingerência no seu conteúdo.

a) O artigo 189.º n.º 1 do Código de Processo Penal

Paulo Pinto de Albuquerque considera que o artigo 189.º n.º 1 CPP estende ao telemóvel o regime das escutas telefónicas, considerando que esta previsão se enquadra no inciso "conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone" [329 e 330]. Há, no entanto, quem entenda que o telemóvel é ainda telefone[331], e que por isso não faz sentido que a extensão operada pelo artigo 189.º n.º 1 CPP se destine ao telemóvel, aplicando-se diretamente o artigo 187.º CPP. Trata-se de uma discussão com pouca amplitude e interesse prático, pois é pacífico que, seja por via direta ou pela norma de extensão, ficou claro que o legislador pretendeu estender o regime das escutas telefónicas ao telemóvel com o artigo 189.º n.º 1 CPP. É por isso pacífico que as chamadas de voz realizadas

[329] Considerando que a extensão se destina ao "telemóvel, teletexto e o videofone", estando excluídos da aplicação do regime das escutas telefónicas o telégrafo, o fax e o telex (sendo aplicável o regime geral das apreensões, consagrado no artigo 178.º CPP) – como se retira de Albuquerque, Paulo Pinto de. *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* 4ª edição. Universidade Católica, 2011. Página 544.

[330] A extensão da aplicação do regime das escutas telefónicas a diversas realidades foi objeto de apreciação da sua conformidade com a Constituição, não tendo sido considerada inconstitucional pelo Tribunal Constitucional no Acórdão 7/87 - disponível em http://www.tribunalconstitucional.pt/tc/acordaos/19870007.html, Processo n.º 302/86; Relator Conselheiro Mário de Brito, acedido e consultado a 26-07-2017.

[331] Como se entendeu no Acórdão do Tribunal da Relação do Porto de 07-07-2010, disponível em http://www.dgsi.pt/jtrp.nsf/-/D81B24CFC47BA41E802577C1004D383C e no Acórdão do mesmo Tribunal de 12-09-2012, disponível em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/877e0322acde18d080257a8300393cc6?OpenDocument, ambos acedidos a 31-07-2017 – ainda que neste último se tenha refletido sobre a necessidade de um novo olhar sobre a temática do acesso a mensagens enviadas e recebidas através do telemóvel após a Lei do Cibercrime.

através do telemóvel podem ser escutadas, tal como as realizadas através do telefone fixo, e estão submetidas ao mesmo regime.

Hoje faz sentido colocar a questão de saber se a definição e funcionalidades de "telemóvel" são equivalentes às que se apresentavam em 1987. Os telemóveis atuais não são em nada equivalentes aos que existiam na década de 80 e 90 do século passado. Hoje são verdadeiros computadores a uma escala mais reduzida, cujas funcionalidades aumentaram exponencialmente. Se até ao início do século o telemóvel servia essencialmente para realizar chamadas de voz e enviar mensagens de texto (e posteriormente, imagem e som, com o aparecimento das *MMS*), hoje pode realizar uma multiplicidade de coisas para além disso: permite a ligação à Internet em qualquer lugar ou momento, o que abre a possibilidade para realização de chamadas através do sistema *Voice Over IP*, o acesso a aplicativos que permitem a troca instantânea de mensagens e ficheiros de imagem, som ou voz, acesso aos diversos servidores de *e-mail* e a qualquer sítio da Internet.

Torna-se assim importante questionar a que segmento de funcionalidade dos "telemóveis" são hoje aplicáveis as escutas telefónicas. Parece claro que continuam sob o regime das escutas telefónicas as chamadas de voz realizadas através dos telemóveis – que em pouco ou nada diferem das chamadas realizadas através do telefone fixo, cujas chamadas motivaram a criação deste regime de "interceção" em primeira mão: trata-se da escuta de conversações faladas e realizadas através de aparelho telefónico, que pela falta de ponderação e reflexão no que é dito, reflete a necessidade da existência de um regime de "interceção" cuidado e exigente.

Questão diferente é a de saber se as mensagens de texto e de imagem enviadas e recebidas através dos telemóveis também se submetem ao regime das escutas telefónicas – fora dos casos em que o destinatário dessas mensagens consinta na sua junção à investigação criminal[332], movendo-se a presente investigação no quadro de meios ocultos de obtenção de prova.

[332] Caso em que é dispensada a intervenção de qualquer autoridade judiciária para a junção dos mesmos aos autos, tal como foi entendido, a título de exemplo, no Acórdão do Tribunal da Relação do Porto de 22-03-2013, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/abf6a7fedb6f7ba580257b88004ed413, acedido a 31-07-2017, pois a aquisição do material probatório não foi realizada por qualquer ação investigatória

Apesar de as *SMS* e as *MMS* integrarem o "serviço telefónico" tal como consagrado na Lei 32/2008, no seu artigo 2.º n.º 1 b)[333], entendemos que a questão não dever ser encarada sob a perspetiva concetual ou do meio através do qual se presta o serviço – no caso, o telemóvel – mas sim tendo em conta a essência da comunicação em si mesma: se é falada, em que se equipara a chamada telefónica através de telefone fixo; ou escrita, que em nada tem comparação com aquela. Ou seja, não é pelo facto de os serviços de mensagens curtas e de multimédia se integrarem na categoria de serviços telefónicos que se devem reconduzir, sem mais, à categoria de "comunicações ou conversações" transmitidas por telefone (para quem entenda que o telemóvel ainda o é) ou por meio técnico diferente do telefone (se se entender que já não cabe neste), a que são aplicáveis as escutas telefónicas.

O que é confirmado pela doutrina e jurisprudência maioritária, que equipara as mensagens de texto e de multimédia ao correio eletrónico, e não às chamadas telefónicas. É exemplo Rita Castanheira Neves, que considera que as *SMS* e *MMS*, ao lado do correio eletrónico, integram a categoria de comunicações eletrónicas escritas, sendo este o elemento que deve produzir a distinção em relação às chamadas telefónicas e impor diferentes catálogos[334] de crimes para os meios de obtenção de prova que se dirijam à ingerência numas ou outras. Esta Autora é clara na tese que propõe: "a aplicação do regime legalmente estabelecido para as escutas telefónicas não se afere pela utilização ou não de um aparelho telefónico. Afere-se, sim, pela pretensão de intercetar e registar conversações telefónicas"[335]

---

das autoridades processuais, não tendo por isso lançado mão de qualquer meio de obtenção de prova – e, por isso, não tendo desrespeitado quaisquer trâmites legais, de que as proibições de prova são a mais penosa cominação – e que se dirigem precisamente às autoridades processuais. No mesmo sentido foi entendido no Acórdão do Tribunal da Relação de Guimarães de 15-10-2012, disponível em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/d7e67584752588c980257aa0004607bc?OpenDocument, acedido a 31-07-2017.
Quando se trata da pesquisa a sistemas informáticos, o artigo 15.º n.º 3 a) LC prevê expressamente que o "órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando a mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado".

[333] Artigo 2.º b) «Serviço telefónico», qualquer dos seguintes serviços: i) Os serviços de chamada, incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados; ii) Os serviços suplementares, incluindo o reencaminhamento e a transferência de chamadas; e iii) Os serviços de mensagens e multimédia, incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhoradas (EMS) e os serviços multimédia (MMS).

[334] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 174.

[335] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 173.

– tese que sufragamos e consideramos como a mais válida para a realização de distinção dos regimes dos meios de obtenção de prova. Assim é porque havendo esta distinção entre o escrito e o falado, é feita a ponderação necessária entre os direitos fundamentais dos indivíduos e os interesses da investigação criminal: quando se trata da ingerência oculta entre conversações faladas há uma maior violação dos direitos fundamentais dos indivíduos, que se expressam na sua plenitude e sem consciência de que estão a perpetuar o que estão a dizer, ao passo que a ingerência em comunicações escritas traz consigo uma compressão de direitos fundamentais menos gravosa, dada a perenidade e reflexão que são inerentes aos escritos, cujo declarante tem conhecimento. Com a Autora podemos afirmar que "a diferente natureza entre as palavras falada e escrita e o subsequente distinto grau de reclamação de proteção deve, pois, conduzir o legislador ordinário a asseverar uma tutela mais inflexível quanto àquela primeira"[336].

Quando à interceção em tempo real de mensagens de texto curtas ou de multimédia, faz sentido remeter-se para o que foi dito em relação à ingerência em tempo real do correio eletrónico enquanto circula na rede, sendo possível esta monitorização e parecendo ser o regime das escutas telefónicas (diretamente ou pela transposição realizada no artigo 18.º LC) o adequado para esse fim.

Quanto ao acesso de mensagens de texto e multimédia que se encontrem armazenadas, enquadram-se no inciso "mesmo que se encontrem guardadas em suporte digital" constante do artigo 189.º n.º 1 CPP: tratam-se de registos em suporte eletrónico do que foi, outrora, comunicação. Já em 2011 Paulo Pinto de Albuquerque considerava que, tratando-se de mensagens arquivadas no cartão do telemóvel, se tratavam de uma "forma de comunicação incluída, por maioria de razão, no âmbito de proteção do artigo 189.º, pelo que a respetiva leitura deve ser autorizada pelo juiz, quer já tenham sido lidas, quer ainda não o tenham sido pelo seu destinatário"[337]. Assim foi entendido no Acórdão do Tribunal da

[336] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 175.

[337] Albuquerque, Paulo Pinto de. *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* 4ª edição. Universidade Católica, 2011. Página 545. Este Autor invoca a título de exemplo a fundamentação constante do Acórdão do Supremo Tribunal de Justiça de 20-09-2006, disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/2e7cf04133dd20f78025723d005a62ab?OpenDocument, acedido e consultado a 31-07-2017: "O cartão do telemóvel é o repositório de mensagens, a

Relação de 15-10-2012[338] – que o cartão *SIM* ou a memória do telemóvel são pacificamente qualificáveis como "suporte eletrónico" ou "digital": "Uma vez aberto o envelope duma carta, esta fica na disponibilidade do destinatário, que a poderá livremente mostrar a quem entender. O mesmo se passa com a sms. Depois de a ler, o dono do telemóvel do destino pode simplesmente apagá-la ou mostrá-la a quem entender. A sms pode continuar a existir no suporte digital do telemóvel enquanto não for apagada, isto é, se for «guardada». Tal como a carta que, depois de lida, pode voltar a ser colocada no envelope, também a sms, igualmente depois de lida, pode continuar guardada em suporte digital".

Costa Andrade entende que sobre as mensagens de texto e de multimédia armazenadas, seja no cartão *SIM* ou no armazenamento do telemóvel não faz sentido estender o regime das escutas telefónicas, uma vez que "o destinatário pode aceder diretamente à mensagem, em relação à qual não subsiste, de resto, nenhum domínio por parte da empresa que oferece o serviço"[339] – que é o fundamento apresentado pelo Autor para justificar a necessidade de aplicação do regime das escutas telefónicas ao correio eletrónico, uma vez que é necessário o ato de "chamada" por parte do destinatário para ter acesso ao *e-mail*, devido ao controlo e domínio que o prestador de serviços continua a deter sobre o correio eletrónico até esse momento.

Nesse sentido foi entendido pelo Tribunal da Relação de Évora, em 07-04-2015[340]: após o trânsito das mensagens pela rede, ou seja, quando são recebidas pelo terminal do

---

respetiva caixa de correio, que as recebe até serem inutilizadas pelo seu destinatário, a mensagem uma forma de telecomunicação, por meio diferente de telefone, à qual se aplicam as regras sobre as escutas telefónicas por força do art.º 190.º, do CPP" [hoje, artigo 189.º CPP].

[338] Disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/d7e67584752588c980257aa0004607bc?OpenDocument, acedido a 31-07-2017.

[339] Como se retira de Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 164.

[340] Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/ad8068a8c8f9b3c080257e2e00356d33?OpenDocument, acedido e consultado a 31-07-2017. No mesmo sentido foi entendido no Acórdão do Supremo Tribunal de Justiça de , disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/21ac26b56cb6b8d6802577a6003109a4?OpenDocument, acedido a 31-07-2017 : "As mensagens que, depois de recebidas, ficam gravadas no recetor deixam de ter a natureza de comunicação em transmissão. São, isso sim, comunicações recebidas, pelo que deverão ter o mesmo tratamento da correspondência escrita já recebida e guardada pelo destinatário. Tal como acontece na correspondência efetuada pelo correio tradicional, diferenciar-se-á a mensagem já recebida mas ainda não aberta da mensagem já recebida e aberta. Na apreensão daquela rege o artigo 179º do C. P. Penal, mas a apreensão da já recebida e aberta não terá mais proteção do que as cartas recebidas, abertas e guardadas pelo

destinatário, deixam de ser consideradas telecomunicação e comunicação em transmissão. Nesse momento "São, isso sim, comunicações recebidas, pelo que deverão ter o mesmo tratamento da correspondência escrita já recebida e guardada pelo destinatário. Tal como acontece na correspondência efetuada pelo correio tradicional, diferenciar-se-á a mensagem já recebida mas ainda não aberta da mensagem já recebida e aberta. Na apreensão daquela rege o artigo 179º do C. P. Penal, mas a apreensão da já recebida e aberta não terá mais proteção do que as cartas recebidas, abertas e guardadas pelo seu destinatário". Consideramos louváveis os argumentos invocados neste aresto para consideração das mensagens como telecomunicação *enquanto* se dá o seu trânsito na rede e a equiparação das mesmas a correspondência tradicional após o seu recebimento, mas há a apontar um argumento que não consideramos correto: foi entendido pelo tribunal que não seria aplicável ao caso qualquer meio de obtenção de prova constante da Lei do Cibercrime pois, "por um lado, não é investigada, nos presentes autos, a prática de qualquer ilícito previsto naquela lei e que, por outro, não está em causa crime cometido por meio de um sistema informático ou crime cuja prova esteja guardada em suportes digitais". Parece haver algum equívoco relativamente à alínea c) do artigo 11.º da Lei do Cibercrime, "Em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico" – trata-se de um perfeito exemplo de investigação em que é necessária a recolha de prova em suporte eletrónico, não se conseguindo perceber qual o obstáculo na integração do cartão *SIM* (*Subscriber Identity Module*) ou a memória do telemóvel na categoria de "suporte eletrónico".

Assim, tal como acontece com o correio eletrónico, é necessária referência à Lei do Cibercrime e aos meios de obtenção de prova nela consagrados, muitas vezes olvidados por doutrina e jurisprudência.

seu destinatário. E a mensagem recebida em telemóvel, atenta a natureza e finalidade do aparelho e o seu porte pelo arguido no momento das revistas e apreensões efetuadas, é de presumir que, uma vez recebida, foi lida pelo seu destinatário. Na sua essência, a mensagem mantida em suporte digital depois de recebida e lida terá a mesma proteção da carta em papel que tenha sido recebida pelo correio e que foi aberta e guardada em arquivo pessoal. Sendo meros documentos escritos, estas mensagens não gozam da aplicação do regime de proteção da reserva da correspondência e das comunicações".

b) A Lei do Cibercrime

Sempre será de questionar, mesmo a entender-se que as mensagens de texto e multimédia enquanto transitam na rede constituem formas de telecomunicação, se o regime das escutas telefónicas é o mais adequado para se regular o acesso a estas mensagens – lembre-se, mesmo que ainda se encontrem em trânsito. Por maioria de razão é também obrigatório questionar se o regime das escutas telefónicas se aplica à "apreensão" de mensagens que já foram recebidas e acedidas pelo destinatário, ou que já estão na sua esfera de acessibilidade.

Nesta matéria é obrigatório chamar à colação os meios de obtenção de prova previstos na Lei do Cibercrime[341]: após a consagração desta Lei, impõe-se ao intérprete e aplicador uma nova reflexão sobre a temática das mensagens de texto e multimédia, enviadas e recebidas através de telemóveis.

Assim, impõe-se uma nota relativa aos meios de obtenção de prova consagrados na Lei do Cibercrime com interesse nesta matéria: existe um meio autónomo para a pesquisa de dados informáticos, no seu artigo 15.º, e a apreensão de correio eletrónico ou de registos de comunicações de natureza semelhante que se afigurem importantes para a investigação quando sejam encontrados no decurso de algum acesso ou pesquisa legítima aos aparelhos informáticos, no artigo 17.º, como *infra* analisado. Se no primeiro se trata da pesquisa "primária" e *per se* aos sistemas informáticos, o segundo destina-se a recolher registos que, por dizerem respeito a comunicações (muitas vezes já lidas, mas podendo conter algumas mensagens por ler, conforme visto) possuem um regime de apreensão distinto dos restantes dados informáticos. Estes meios de obtenção de prova são aplicáveis à investigação de crimes previstos na Lei do Cibercrime ou em qualquer outro normativo, desde que sejam "cometidos por meio de um sistema informático, ou "em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico". Para além destes, existe o artigo 18.º LC, que consagra a interceção de comunicações, que veremos se é ou não aplicável às mensagens curtas de texto e multimédia.

[341] Tal como foi entendido no Acórdão do Tribunal da Relação do Porto de 12-09-2012, disponível em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/877e0322acde18d080257a8300393cc6?OpenDocument, acedido a 31-07-2017.

Como a generalidade dos Autores e jurisprudência portuguesa, consideramos que as mensagens curtas de texto se assemelham ao correio eletrónico, não fazendo sentido fazer-se distinção entre o regime de um e outro. Quanto às mensagens multimédia, apesar de não constituírem mensagens escritas, em tudo se assemelham ao correio eletrónico, pois trata-se da transmissão de quaisquer imagens, sons ou ficheiros[342]. Desta forma, o inciso "ou de registos de comunicações de natureza semelhante" constante do artigo 17.º LC é perfeitamente subsumível às mensagens de texto e multimédia constantes de qualquer armazenamento informático, fazendo com que o acesso ao seu conteúdo possa ser realizado em qualquer tipo de crime, e não apenas no catálogo previsto para as escutas telefónicas.

Reproduzimos na íntegra tudo o que foi dito em relação ao correio eletrónico, tratando-se as mensagens de texto curtas e de multimédia formas de comunicação escrita, em que sempre é feita pelo interlocutor a reflexão e ponderação necessárias no que é "dito" (escrito) ou dos ficheiros a enviar, não se tratando de uma forma de comunicação instantânea, que sempre mediará algum tempo (ainda que o envio e receção do correio eletrónico seja feita de forma praticamente instantânea, não é comum estabelecer-se conversações através do *e-mail*, até pelo surgimento de aplicativos mais indicados para tal, como veremos).

Assim, é de considerar, em suma, que: é aplicável à pesquisa *per se* de mensagens curtas ou multimédia o meio de obtenção de prova consagrado no artigo 15.º LC, tratando-se de dados informáticos armazenados em suporte digital (no cartão *SIM* do utilizador, em qualquer cartão de memória ou no telemóvel destinatário[343]); uma vez detetadas mensagens arquivadas através das pesquisas, é aplicável às mensagens curtas e de multimédia a apreensão dos seus registos, consagrada no artigo 17.º LC, tratando-se de registos de natureza semelhante ao correio eletrónico – sem ser realizada a distinção relativamente ao conhecimento, ou não, do conteúdo da mensagem pelo destinatário, tal como visto anteriormente e devido ao facto de o legislador assim o consagrar expressamente. É

[342] No mesmo sentido entende Rita Castanheira Neves, em Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 178.

[343] Tal como foi entendido no Tribunal Relação de Guimarães de 29 de março de 2011, relator: Maria José Nogueira, disponível em http://www.dgsi.pt/JTRG.NSF/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument, acedido a 18-08-2017: "o que se pretende é aceder a um documento (pois que é isso de que se trata, quando se fala de dados informáticos subsumíveis á categoria de SMS), que se encontra guardado digitalmente, ou seja, num sistema informático (no caso, um sistema composto por hardware, a parte física do telemóvel, e software, o programa informático que descodifica os sinais em que se encontram armazenados diretamente na "memória" do telemóvel ou virtualmente na rede a que acede o cartão SIM)."

igualmente aplicável a "interceção de comunicações" prevista no artigo 18.º LC, quando a investigação criminal necessite de monitorizar, em tempo real, as mensagens de texto e multimédia enquanto transitam na rede de telecomunicações, até alcançarem o terminal de destino.

5. As mensagens instantâneas

Com o desenvolvimento da tecnologia têm surgido, ao longo dos tempos, novas e múltiplas formas de comunicar e interagir com os outros, ainda que nos lugares mais recônditos do mundo, e cada vez com menos custos, mais rapidez e precisão, através da Internet, a Rede das Redes.

Surgem assim aplicações como o *Facebook Messenger*, *WhatsApp*, *GoogleTalk*, e *Sykpe,* que permitem a troca de mensagens de texto, imagem ou som de forma instantânea, em que são frações de segundos que medeiam o envio e receção das mensagens, possibilitando conversações em tempo real, em muito semelhantes às mantidas oralmente, mas que se processam seja por forma escrita, seja através de imagens, sons, vídeos, etc. Tratam-se de programas informáticos em que os interlocutores conseguem manter um diálogo em tempo real, através da velocidade da Internet, sendo inclusivamente possível aos interlocutores saber ao segundo quando o outro receciona, lê a mensagem e até quando escreve alguma resposta, mesmo sem a enviar. É também possível saber se o interlocutor optou por não abrir/ler a mensagem (sempre que é aberta, é presumivelmente lida), apesar de ter acedido ao programa informático posteriormente ao envio da mesma. Atualmente muitas das aplicações informáticas permitem a codificação ou encriptação das mensagens ou chamadas que realizam, o que faz com que apenas os interlocutores possam ter acesso à conversa e às mensagens enviadas e recebidas[344]. Disso é exemplo o caso do *WhatsApp*, que é utilizado por mais de mil milhões de pessoas[345], que realiza um sistema de encriptação "ponta-a-ponta", e cujo objetivo é garantir a total confidencialidade das mensagens enviadas

[344] Como se retira de Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 164.

[345] Conforme notícia disponível em https://www.rtp.pt/noticias/mundo/falha-no-whatsapp-permite-espionagem-de-mensagens-encriptadas_n975797, acedida a 24-08-2017.

e recebidas, a que nem o prestador de serviços teria acesso[346]. Também o *Facebook Messenger* possui a possibilidade de encriptação de mensagens[347], aplicação que é utilizada por mais de novecentos milhões de pessoas.

Consideramos que se trata de uma forma de comunicação distinta do correio eletrónico ou até mesmo da troca de mensagens de texto e de multimédia: parece-nos que não assiste aos interlocutores a reflexão que cunhariam num *e-mail* ou mensagem de texto, mas antes se exprimem como se o fizessem oralmente, dada a instantaneidade de emissão da mensagem e possibilidade de leitura, em que se vai escrevendo à medida que se vai pensando, tal como se vai dizendo à medida que se pensa. Assim, trata-se de uma forma de comunicar que mais se assemelha a conversações orais apesar da sua forma escrita, devido à instantaneidade que é a marca destas aplicações.

No entanto, não devemos esquecer que estas conversações se processam de forma escrita, que é o aspeto que consideramos mais importante na aferição do regime para a obtenção da prova – ainda que possuam características, na conversação em si, semelhantes às mantidas por via oral, devem ser equiparadas ao regime de recolha do correio eletrónico, pois não se poderia pensar num ordenamento jurídico que consagrasse meios de obtenção de prova específicos para cada possibilidade técnica de comunicação: seria um rombo na sistemática e contrária à teoria geral de meios ocultos de obtenção de prova que *infra* defendemos, bem como ao grande critério delimitador que consideramos fundamental, a natureza da comunicação em que a investigação criminal se pretende imiscuir.

A grande maioria dos Autores que refletiu sobre estes temas considera que estas mensagens devem ser equiparadas ao *e-mail*, remetendo para o regime deste a ingerência naquelas. Assim o faz Pedro Dias Venâncio, no que toca à "interceção" em tempo real do correio eletrónico enquanto circula na rede: se o artigo 18.º LC se aplica ao correio eletrónico, também se aplica à "interceção de mensagens trocadas através de processos de comunicação

[346] O que tem vindo a ser desmentido através de várias notícias, sendo possível que exista uma "porta dos fundos" suscetível de permitir o acesso ao conteúdo das mensagens, como se retira, a título de exemplo, de https://www.publico.pt/2017/01/13/tecnologia/noticia/whatsapp-mensagens-encriptadas-podem-ser-espiadas-1758170, acedido a 24-08-2017.

[347] Como se retira do próprio site do *Facebook:* https://www.facebook.com/help/messenger-app/1084673321594605/?helpref=hc_fnav, acedido a 24-08-2017.

instantânea (usualmente designados por serviços de "Chat", como são os casos do "IRC" do "MSN Messenger" ou do "ICQ")"[348 e 349].

Paulo Pinto de Albuquerque, relativamente à "interceção em tempo real" destas mensagens, considera que a "interceção de mensagens trocadas por serviços de comunicação instantânea (chat), como o MSN Messenger, ou até de comunicações áudio realizadas através de voice over IP"[350] apenas pode ter lugar nos crimes do catálogo do artigo 187.º CPP, respeitados os trâmites do artigo 188.º CPP – pela mão do artigo 189.º n.º 1 CPP. Parece ter sido a mesma a consideração do legislador quando consagrou o artigo 18.º LC, apesar de ter ainda incluído no catálogo os crimes previstos na Lei do Cibercrime.

Costa Andrade, ainda que se dirigindo às chamadas realizadas através da Internet, as chamdas *VoiceOverIP*, entende que a interceção de comunicações eletrónicas enquanto circulam na Internet é inútil devido à encriptação ou codificação que muitos programas utilizam, já que a mensagem apenas é descodificada para leitura no terminal do destinatário[351]. Este Autor considera que o meio mais útil para a ingerência no conteúdo destas comunicações parece ser a "vigilância nas fontes" – ou seja, a investigação criminal imiscuir-se no próprio computador ou em qualquer aparelho informático do destinatário e realizar a monitorização das conversações por ele realizadas e recebidas sem que ele disso se aperceba. No entanto, trata-se de um tema ainda em discussão, que muitos consideram ser de rejeitar devido aos perigos que isso acarreta para os direitos fundamentais dos indivíduos, bem como no momento de traçar limites à investigação criminal e aos elementos que se investiga[352].

Assim, neste momento podemos afirmar que, em abstrato, a "interceção de comunicações" prevista no artigo 18.º LC é aplicável à "monitorização" das comunicações

---

[348] Venâncio, Pedro Dias. *Lei do Cibercrime anotada e comentada.* 1ª. Coimbra Editora, 2011. Página 119.
[349] No mesmo sentido entende Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017. Página 76.
[350] Albuquerque, Paulo Pinto de. *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* 4ª edição. Universidade Católica, 2011. Página 544.
[351] Como se infere de Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 165.
[352] Apesar de possuir todo o interesse para a investigação criminal, não nos propusemos com a presente investigação a criação/consagração de novos meios de obtenção de prova, apenas à tentativa de compreensão dos meios de obtenção de prova existentes e que regem, afinal, a ingerência no conteúdo das comunicações eletrónicas. Para mais desenvolvimentos sobre o tema consultar, entre outros, Ramalho, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Almedina, 2017.

eletrónicas instantâneas enquanto circulam na Internet. Se o aplicativo realizar a encriptação das mensagens/sinal de voz e não for possível descodificar o seu conteúdo, sempre se poderá ter acesso aos dados externos à comunicação, como sejam os dados de tráfego, base e localização. Assim, detetando-se mensagens relativas a conversações permitidas através de tais programas informáticos que realizem a encriptação das mesmas, poder-se-á recorrer à apreensão dos registos e das mensagens ainda não lidas através do meio de obtenção de prova previsto no artigo 17.º LC[353].

Questão diferente é a de saber qual o regime a aplicar à ingerência no conteúdo das comunicações eletrónicas instantâneas armazenadas em dispositivos informáticos, sem que se pretenda a monitorização do seu transito em tempo real – ou seja, quando não estão em trânsito pela rede e se encontram nos aparelhos informáticos dos interlocutores, ou na bae de dados do servidor.

Vejamos qual o regime de ingerência no conteúdo destas comunicações. Parece que é possível a realização de pesquisas informáticas a computadores, *tablets* ou telemóveis que respeitem os trâmites do artigo 15.º LC, pois visam a pesquisa de dados informáticos armazenados no computador.

Realizadas as pesquisas e encontrando-se mensagens instantâneas, enviadas e recebidas pelos programas enunciados a título de exemplo, deve reger o regime do artigo 17.º LC para a sua recolha para a investigação criminal, uma vez que se tratam de "registos de comunicação semelhantes" ao correio eletrónico: apesar de ser diferente o grau de ponderação que vai implicado no envio de um *e-mail* e de uma mensagem neste tipo de aplicações e conversações, não poderia pensar-se num regime próprio para estas comunicações, constituindo de facto "registos" do que outrora foi comunicação, e não se poderia pensar num regime sem ter em conta a sua forma escrita – elemento que mais deve relevar. Para concluir, não deve ser o regime das escutas telefónicas a regular a sua recolha para a investigação criminal, tal como indicia o artigo 189.º n.º 1 CPP, mas sim o artigo 17.º

[353] Com interesse neste ponto figura o "relatório sobre pedidos governamentais" portugueses relativo ao Facebook, respeitante ao período de Julho de 2016 e Dezembro de 2016, disponível em https://govtrequests.facebook.com/country/Portugal/2016-H2/, acedido a 25-08-2017, em que é possível verificar que de em 737 pedidos em processos judiciais, apenas foram apresentados dados em 52.78% dos mesmos.

LC – para além da substancial diferença do catálogo de crimes a que é aplicável, a nível hermenêutico é a solução com mais sentido.

Sem esquecer que o artigo 17.º LC disciplina o meio de obtenção de prova nele consagrado sem efetuar a distinção entre as mensagens (correio eletrónico, mensagens de texto e multimédia e instantâneas) cujo conteúdo já foi conhecido pelo destinatário e o que ainda não o foi. Por isso, sendo descobertas pela investigação criminal mensagens instantâneas em qualquer dispositivo informático, o seu conteúdo deve ser recolhido para a investigação criminal através dos trâmites do artigo 17.º LC.

6. As chamadas de voz realizadas através do sistema "Voice Over IP"

A Internet, para além de possibilitar o envio e receção de mensagens de texto, som, imagem ou vídeo de forma instantânea, permite também a realização de chamadas através do IP (*Internet Protocol*). Assim, o sistema *Voice Over IP*, "permitindo chamadas áudio, de qualidade similar às chamadas telefónicas, com possibilidade de ligação entre computadores ou de computadores para redes telefónicas fixas ou móveis, e com custos para o utilizador consideravelmente mais baixos que as comunicações telefónicas, está em exponencial crescimento a nível mundial"[354].

Ensina Costa Andrade que "os serviços *VoIP* convertem a voz em sinal digital, que circula através da *internet* e que é convertido de novo em voz imediatamente antes de chegar ao aparelho de destino. Para o efeito pode utilizar-se o computador, um telefone especial, próprio para *VoIP*, ou um telefone normal com a interposição de um *modem*. Para além de circular em sinal digital, a conversação é feita, cada vez mais, de forma codificada ou críptica, de tal modo que só os próprios interlocutores podem seguir a conversa"[355]. Ou seja, as aplicações informáticas garantem[356] a confidencialidade das conversações, impedindo a ingerência dos prestadores de serviços e de terceiros, que não os intervenientes na conversação. A conversação é, em tudo, semelhante às mantidas através de um telefone ou

[354] Venâncio, Pedro Dias. *Lei do Cibercrime anotada e comentada.* 1ª. Coimbra Editora, 2011. Página 119.
[355] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 164.
[356] Confrontar com nota 356 – afinal, podem proteger a conversa de terceiros e possibilitar a estes o seu acesso?

de um telemóvel, apenas diferindo o meio técnico através do qual se processa, e da possibilidade técnica de encriptação que lhe assiste quando realizada através da Internet. Costa Andrade considera que a "interceção", pretensa "escuta" da conversação enquanto circula na rede, é inútil, uma vez que a voz é convertida em sinal digital, não se conseguindo ter acesso ao conteúdo do que é transmitido. Por isso faz o Ilustre Autor apelo à "vigilância nas fontes", que possibilitaria a captação das "palavras do emitente antes da codificação, ou as do destinatário depois da descodificação", "o que se faz ou através de microfone oculto ou infiltrando os computadores através de adequados programas do género «cavalo de Tróia»"[357].

A conclusão do regime a aplicar à ingerência no conteúdo destas conversações não carece de grandes rodeios, face a tudo o que ficou exposto até aqui: tratando-se de conversações de voz, deve ser aplicável o regime das escutas telefónicas, pois trata-se da ingerência na mesma realidade, o conteúdo das conversações orais. Assim o defendemos ao longo da presente investigação: o meio de obtenção de prova a consagrar ou destinar à ingerência no conteúdo das comunicações eletrónicas deve ser pautado pelo critério da comunicação em si – se falada ou escrita, e não pelo meio técnico através do qual a comunicação é realizada. Nesse sentido entende Rita Castanheira Neves: "efetivamente, não pode ser o facto de se tratar de um telefone ou, ao invés, da *Internet*, que permite estabelecer a distinção entre diferentes meios de obtenção de prova, com os correspondentes diferentes regimes de regulamentação. Se através da *Internet* se estabelece uma conversa telefónica, por exemplo por via do programa *Skype*, não haverá duvidas de que a interceção que se lhe impuser terá de cumprir os requisitos legais estabelecidos no regime das escutas telefónicas"[358].

Assim foi consagrado no artigo 18.º da LC: em que se restringe o catálogo de crimes a que é aplicável o meio de obtenção de prova, nomeadamente de falsidade informática (artigo 3.º), de dano relativo a programas ou outros dados informáticos (artigo 4.º), de sabotagem informática (artigo 5.º), de acesso ilegítimo (artigo 6.º), de interceção ilegítima

[357] Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009. Página 165.
[358] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 172.

(artigo 7.º), de reprodução ilegítima de programa protegido (artigo 8.º), e de perda de bens (artigo 10.º), para além dos "crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico", quando se trate dos crimes previstos no número 1 do artigo 187.º CPP[359].

7. O imbróglio legislativo e a luz ao fundo do túnel

Como visto ao longo da presente investigação, convivem no ordenamento português diferentes normativos relativamente à ingerência, pela investigação criminal, no conteúdo das conversações eletrónicas mantidas através da Internet.

O mítico artigo 189.º n.º 1 CPP reflete as várias oportunidades que foram perdidas para a sua eliminação, pelo menos desde a entrada em vigor da Lei do Cibercrime, em 2009 – que se destina aos crimes informáticos, mas, mais do que isso, à recolha de prova em suporte eletrónico na investigação de qualquer crime. Por isso o artigo 11.º da LC contém um amplíssimo catálogo de crimes a que os meios de obtenção de prova contidos na Lei do Cibercrime são aplicáveis: "a pretensão do legislador (quer o nacional quer o convencional) é o de, declaradamente, alargar o âmbito da aplicação da lei até onde haja necessidade de fazer prova com o conteúdo existente em qualquer sistema informático"[360].

Ao mesmo tempo que a Lei do Cibercrime prevê meios de obtenção de prova específicos para a criminalidade informática e para a recolha de prova na investigação de qualquer crime, quer seja cometido por meio de um sistema informático ou em que seja necessário recolher à prova em suporte eletrónico (com exceção da interceção de

[359] Nomeadamente, os do número 1: "a) Puníveis com pena de prisão superior, no seu máximo, a 3 anos; b) Relativos ao tráfico de estupefacientes; c) De detenção de arma proibida e de tráfico de armas; d) De contrabando; e) De injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone; f) De ameaça com prática de crime ou de abuso e simulação de sinais de perigo; ou g) De evasão, quando o arguido haja sido condenado por algum dos crimes previstos nas alíneas anteriores.".

[360] Conforme se retira do Acórdão do Tribunal da Relação de Évora de 20-01-2015, relator: João Gomes de Sousa, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument, acedido a 25-08-2017.

comunicações e ações encobertas, conforme o artigo 11.º LC), permanece no Código de Processo Penal uma "casa dos horrores hermenêutica", que prevê soluções diferentes para a recolha das mesmas provas – que permanece inalterado, mesmo depois de o legislador consagrar "novos" regimes, ou optar por diferentes soluções.

É exemplo flagrante o caso do correio eletrónico: a sua ingerência – seja em tempo real, seja pela vertente do acesso aos seus registos, tem de respeitar o regime e trâmites das escutas telefónicas pela mão do artigo 189.º n.º 1 CPP, ao passo que, pelo menos quanto ao acesso aos seus registos, é aplicável regime semelhante ao da apreensão da correspondência, conforme o artigo 17.º LC. O mesmo entende Benjamim da Silva Rodrigues: "O que significa que há uma encruzilhada – e uma nova face oculta – nesta matéria, pois o correio eletrónico continuará a fazer o seu constrangedor e confrangedor curso, na doutrina e jurisprudência, umas vezes como comunicação eletrónica (ou antigamente «telecomunicação») a levar ao altar das escutas telefónicas, outras vezes como comunicação eletrónica a levar ao altar da correspondência clássica, outras vezes como amálgama de dados a levar ao altar das escutas telefónicas e, por último, enquanto dados a implicar outros de tráfego e, por isso, fazer intervir a legislação específica da Lei 32/2008"[361].

Também Conde Correia aponta as dificuldades interpretativas e de aplicação geradas pela existência de leis não harmonizadas nem consentâneas no ordenamento jurídico português: "Esta trilogia (CPP, Lei 32/2008 e Lei do cibercrime), para além de acentuar o atual paradigma da 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 de nefasto insucesso prático"[362]. São evidentes as dificuldades que a multiplicidade de normativos sobre as mesmas realidades produzem na sua aplicação e interpretação, o que põe em causa a justiça e os direitos fundamentais dos cidadãos, num Estado de Direito – o que é agravado quando as soluções são diferentes. Com Paulo Dá Mesquita, podemos afirmar que "Os espaços de dúvida e indefinições no tecido normativo sobre a prova eletrónica e telecomunicações no direito processual português

[361] Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011. Página 532.
[362]Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 30.

multiplicam as áreas de opacidade normativa. Além das dificuldades dos juristas acederem a uma fenomenologia diferente daquela em que estabeleceram os seus cânones e pré-compreensões sobre os mundos do direito e da vida, emerge o problema da natureza difusa das fronteiras e previsões normativas e das próprias divisões de competências judiciárias e processuais"[363].

Resta por isso tentar traçar um rumo de compreensão dos meios de obtenção de prova dirigidos à ingerência no conteúdo das comunicações eletrónicas, possibilitadas através da Internet, para evitar que, "em cada situação concreta, o julgador deverá pois – num dispensável exercício de verdadeiro equilibrismo jurídico – verificar qual o regime processual aplicável, partindo depois para a sua interpretação"[364].

Assim, conforme Rita Castanheira Neves, podemos afirmar que "a interceção de correio eletrónico, na sua fase de transmissão, em todas as investigações em que esteja em causa um crime informático ou um crime do artigo 187.º mas em que haja necessidade de recorrer à recolha de prova em suporte eletrónico, far-se-á, não diretamente segundo o regime das escutas telefónicas, com base na remissão estabelecida no artigo 189.º do Código de Processo Penal, mas já por aplicação das regras definidas na nova Lei do Cibercrime. Por outro lado, se é verdade que a interceção de comunicações em tempo real consagrada na Lei do Cibercrime não modifica em quase nada o regime consagrado para as escutas telefónicas, para o qual, aliás, remete – ultrapassando ainda a dificuldade prático-jurídica que impedia o recurso a esta diligência na investigação de crimes onde era mais premente –, já no que concerne à ingerência nas comunicações armazenadas, a Lei do Cibercrime vem instituir um verdadeiro novo regime jurídico, concretizando, ainda que em parte, a necessidade de autonomização de regime de que se começou a falar em 1998, mas que se tornou imperiosa depois da Reforma de 2007"[365]. Também Pedro Verdelho o considera: "este regime especial [artigo 18.º LC] não revogou o previsto no art. 189.º CPP nem colide com o mesmo, limitando-se a criar um regime específico, de âmbito limitado aos crimes descritos na Lei do

[363] Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010. Página 124.
[364] Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 37.
[365] Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011. Página 285.

Cibercrime. Desta forma, o regime do art.189.º mantem-se em vigor para todos os restantes casos"[366].

No entanto, é importante relembrar que o artigo 189.º n.º 1 CPP não se limita a remeter para o regime das escutas telefónicas a monitorização em tempo real da transmissão de correio eletrónico, de mensagens de texto, multimédia, ou instantâneas: ele estende do mesmo modo o regime das escutas telefónicas aos registos destas comunicações, que nada têm que ver com "interceção" de comunicações em tempo real – seja na vertente de "comunicações" (que os registos nunca poderão ser), nem "em tempo real" (pois ao aceder-se a registos, não se trata de uma operação que se ingere em informações/comunicações transmitidas "em tempo real", apenas através da sua monitorização enquanto circula na rede).

Ou seja, após a consagração do artigo 17.º LC há uma clara perda de conteúdo útil do artigo 189.º n.º 1 do CPP, que deixa de ser aplicável à "interceção" de correio eletrónico, restantes comunicações e registos das mesmas. Para isso consagrou o legislador, no artigo 11.º da LC um amplíssimo catálogo de crimes a que este meio de obtenção de prova é aplicável. A não entender-se assim, seria admitir que a investigação de determinados crimes, considerados como os mais graves e presentes no catálogo das escutas telefónicas possui um regime mais dificultado na recolha do conteúdo de correio eletrónico e demais comunicações eletrónicas, naturalmente armazenados em sistemas informáticos, tendo a investigação de respeitar os trâmites das escutas telefónicas (previstos nos artigos 187.º, 188.º e 190.º CPP), ao passo que a generalidade dos crimes em que seja necessária essa mesma prova pode ver a mesma ser recolhida para a sua investigação respeitando trâmites menos onerosos, constantes no artigo 17.º LC.

Assim, podemos concluir que a interceção em tempo real das comunicações eletrónicas sempre se fará seguindo o regime das escutas telefónicas, pela mão do artigo 18.º LC, e não do artigo 189.º CPP, ao passo que a apreensão de correio eletrónico e demais comunicações eletrónicas será feita através do artigo 17.º LC.

Com o esvaziamento de conteúdo útil do artigo 189.º n.º 1 CPP reclamam-se modificações no ordenamento jurídico português. Não se compreende o motivo da

[366] Verdelho, Pedro. "A nova Lei do Cibercrime." *Scientia Iuridica*, Outubro-Dezembro de 2009, n.º 320. Página 747.

permanência desta norma de extensão no Código de Processo Penal, pois na realidade existem normativos que consagram soluções expressas para a obtenção das provas a que aquele se destinava. É também incompreensível a consagração de meios de obtenção de prova que se dirigem à investigação de quaisquer crimes em lei especial, nomeadamente na Lei do Cibercrime, pelo que faria mais sentido e levaria a menos confusões interpretativas que estes figurassem no Código de Processo Penal, no capítulo relativo aos meios de obtenção de prova: Título III do Livro III, sendo uma solução possível a consagração de um capítulo relativo à obtenção de prova em suporte eletrónico.

Para além desta autonomização fora do Código de Processo Penal, alguns problemas foram apontados às soluções consagradas, nomeadamente no que diz respeito à opção pela falta de diferenciação entre as mensagens correio e demais comunicações eletrónicas já lidas e as que ainda não o foram, pelo que, a nosso ver, se reclama a intervenção legislativa para adequação da solução a dar ao correio eletrónico já lido – a que deve corresponder um regime de obtenção de prova semelhante ao destinado à apreensão de documentos físicos normais. Com Conde Correia, afirmamos que "As leis do cibercrime revelam ambos os defeitos: são más leis e são insuficientes, estando na hora de ser alteradas. A experiência e o conhecimento adquiridos já permitem superar as suas deficiências e criar um sistema que, sem esquecer o nível ideal de proteção dos direitos fundamentais, contribua para a eficácia da justiça penal"[367].

[367] Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 59.

Conclusão

A Sociedade da Informação afirmou-se desde a década de 70 do século passado. Um dos seus pilares é a Internet, cuja importância no dia-a-dia dos cidadãos é inegável, já que a ela recorrem em todos os domínios da sua vida. Atualmente, devido à grande velocidade de transmissão, cobertura mundial e reduzidos custos, os indivíduos recorrem diariamente a aplicações informáticas que lhes permitem comunicar com quem quer que seja, situando-se em qualquer parte do globo.

Foi assim sendo alterado o paradigma comunicacional e informacional, afirmando-se as comunicações eletrónicas, realizadas através da Internet: chamadas de voz e imagem através do sistema de *Voice over IP* (de que são exemplo o *Skype* e o *FaceTime*), o correio eletrónico e as mensagens instantâneas trocadas através de aplicações como *Facebook Messenger* ou o *WhatsApp*. Têm ainda relevância as mensagens de texto e multimédia que são enviadas e recebidas através dos telemóveis, que, apesar de terem perdido alguma importância face ao desenvolvimento da Internet, continuam a ser bastante utilizadas.

Desde cedo que a investigação criminal percebeu os benefícios que poderia ter a ingerência secreta no conteúdo das comunicações dos indivíduos, como modo de recolher para si informações imperiosas para desvendar as questões levantadas pela prática de crimes – principalmente as que estes pretendem que sejam transmitidas a um ou mais destinatários concretos, coexistindo assim diversos meios ocultos de obtenção de obtenção de prova no ordenamento português.

No entanto, qualquer meio de obtenção de prova consagrado, ou que se pretenda consagrar, apenas pode ser admissível se realizada a necessária ponderação entre os direitos fundamentais dos indivíduos que serão comprimidos pelos interesses da investigação criminal: afinal, "a eficácia da Justiça é também um valor que deve ser perseguido, mas, porque numa sociedade livre os fins nunca justificam os meios, só é aceitável quando alcançada lealmente, pelo engenho e arte, nunca pela força bruta, pelo artifício ou pela mentira, que degradam quem os sofre, mas não menos quem os usa"[368]. Assim é pois estão

[368] Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010. Página 736.

em causa direitos fundamentais tais como o direito à reserva da intimidade privada; o direito à palavra falada, que possui maior proteção constitucional que a palavra escrita, devido à maior volatilidade e menor reflexão no que é dito; o direito à inviolabilidade do domicílio e da correspondência, em especial das telecomunicações e demais meios de comunicação, que em última instância assegura o direito à privacidade e ao livre desenvolvimento da personalidade; o princípio contra a não-autoincriminação, que impede a consagração de meios de obtenção de prova que levem os investigados a proferir palavras ou atos que provoquem a sua própria inculpação; e o direito à autodeterminação informacional, que se vem afirmando ao longo dos anos com a crescente informatização dos dados dos indivíduos, de quaisquer natureza. Estes direitos sofrem exponenciais violações quando se considerem meios de obtenção de prova que se processem de forma secreta, sem que os visados disso tenham conhecimento ou prestem o seu conhecimento – que, aliás, é o motivo da sua eficácia.

Para além disso, se a investigação criminal realizar a ingerência no conteúdo das comunicações dos indivíduos sem respeitar os trâmites legais consagrados (ou não) para tal, incorre, tal como qualquer indivíduo, nos crimes de "violação de correspondência ou de telecomunicações", constante do artigo 194.º do Código Penal, de "devassa por meio de informática", artigo 193.º do Código Penal, bem como de "interceção ilegítima" em sistemas informáticos, previsto no artigo 7.º da Lei do Cibercrime.

Quanto aos meios ocultos de obtenção de prova que se dirijam à ingerência no conteúdo das comunicações privadas dos indivíduos, parece que no ordenamento português tem lugar de destaque o instituto das escutas telefónicas, que podem ser apontadas como a sua "primeira forma" e o regime chapéu de todos os métodos ocultos. Assim é devido à ação do artigo 189.º n.º 1 do Código de Processo Penal, que estende a aplicação do regime processual das escutas telefónicas à ingerência nas "conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presentes".

Como é facilmente percetível, e no que à presente investigação diz respeito, parece que o legislador processual, através da malograda "casa dos horrores hermenêutica", pretendeu estender o regime das escutas telefónicas (pensado para a "escuta" de chamadas

telefónicas necessariamente orais), a uma multiplicidade de realidades que em pouco se assemelham à palavra intercetada em chamada telefónica. Assim, atentando no artigo 189.º n.º 1 do Código de Processo Penal, parece que o regime das escutas telefónicas se aplica também à ingerência no *conteúdo* do correio eletrónico ou de "outras formas de transmissão de dados por via telemática" – que se tratam de comunicações e transmissões de dados que assumem a forma escrita e por isso perene, elemento que retira o sentido de tal ingerência possuir um regime processual tão exigente como aquele em que se pretende imiscuir em comunicações privadas orais. Para além disso, o artigo 189.º n.º 1 do Código de Processo Penal estende o regime das escutas telefónicas ao acesso aos registos do que foi, outrora comunicação – o que não se percebe, visto constituírem registos já tratados e arquivados pelo destinatário, em tudo semelhantes a documentos físicos.

No entanto, desde 2009, com a consagração da Lei do Cibercrime, o intérprete e aplicador não pode ater-se à simples análise e consideração do artigo 189.º n.º 1 do Código de Processo Penal. É que esta Lei não diz respeito apenas à "cibercriminalidade", mas possui um espectro bastante mais amplo: dirige-se à recolha de prova em suporte digital, consagrando diversos meios de obtenção de prova tal, estatuindo inclusivamente diferentes soluções em relação às plasmadas no artigo 189.º n.º 1 do Código de Processo Penal. Os que interessam para a presente investigação, contendentes com a ingerência nas comunicações eletrónicas, e consequentemente, nos seus registos, encontram-se previstos no artigo 15.º – "pesquisa de dados informáticos", no artigo 16.º – "apreensão de dados informáticos", artigo 17.º – "apreensão de correio eletrónico e registos de comunicações de natureza semelhante", e artigo 18.º – "interceção de comunicações.

Após termos constatado algum desprezo da *praxis* judiciária pela Lei do Cibercrime e pelos meios de obtenção de prova nela consagrados, de que o imutável artigo 189.º do Código de Processo Penal é pedra de toque (apesar de diversos alertas doutrinários), consideramos que se impõe uma tentativa de "esquematização" dos regimes que regem, afinal, os meios de obtenção de prova que se dirigem à ingerência no conteúdo das comunicações eletrónicas, possibilitadas pela Internet.

Em relação ao correio eletrónico, pudemos concluir que à sua apreensão é aplicável o meio de obtenção de prova consagrado no artigo 17.º da Lei do Cibercrime, deixando de

lhe ser aplicável o regime das escutas telefónicas pela extensão operada pelo artigo 189.º n.º 1 CPP. A recolha do correio eletrónico para a investigação criminal pauta-se assim por regime, que, a final, remete para o regime da apreensão da correspondência, não sendo feita a distinção entre o correio eletrónico que foi aberto e lido pelo destinatário e o que não o foi – ponto que discordamos, uma vez que a ingerência em correio eletrónico que ainda não foi conhecido pelo seu destinatário é uma violação potencialmente mais gravosa dos seus direitos fundamentais do que a ingerência em correio eletrónico cujo conteúdo já é conhecido pelo destinatário, que se trata, aliás, de registos já tratados e armazenados, que poderiam facilmente ser apreendidos como qualquer outro dado informático, pela mão do artigo 17.º. Quanto à monitorização do correio eletrónico enquanto circula na rede, consideramos ser de aplicar o artigo 18.º da Lei do Cibercrime, tal como se entendia até à consagração desta Lei ser de aplicar ao regime das escutas telefónicas. Quanto aos ficheiros anexos ao correio eletrónico, consideramos que devem beneficiar do mesmo regime de acesso e recolha que o correio eletrónico em si, nos casos em que for percetível a ligação dos mesmos ao correio eletrónico. No entanto, quando ficheiros e correio eletrónico em si forem autonomizados em qualquer local do sistema informático e não for possível estabelecer qualquer ligação entre eles, os ficheiros devem ser tratados como quaisquer outros, e recolhidos para o processo através do mecanismo previsto no artigo 16.º da Lei do Cibercrime.

Quanto às mensagens de texto e multimédia, é de concluir que se deve aplicar o mesmo regime que rege a pesquisa, acesso e recolha do correio eletrónico para o processo criminal, dado que possuem todas as características que as equiparam aquele, como sejam a forma escrita e a necessária ponderação no que vai escrito, afastando-se do reduto caracterizador das chamadas telefónicas: as conversas orais mantidas através de aparelho telefónico.

Relativamente às mensagens instantâneas possibilitadas através da Internet, apesar de possuírem as características de volatilidade e pouca reflexão no que é dito/escrito, não deixam de possuir a forma escrita e como tal deve a sua ingerência ser pautada pelo mesmo regime da apreensão do correio eletrónico, artigo 17.º da Lei do Cibercrime – e a sua monitorização enquanto circula na rede pelo mecanismo previsto no artigo 18.º da Lei do Cibercrime.

Tratando-se de chamadas efetuadas através do sistema *VoiceOverIP*, sendo de conversações de voz, consideramos que deve ser aplicável o regime das escutas telefónicas, pois trata-se da ingerência na mesma realidade, o conteúdo das conversações orais. Aplica-se assim a "interceção de comunicações" prevista no artigo 18.º da Lei do Cibercrime, que subsidiariamente remete para a aplicação do regime das escutas telefónicas.

É assim de concluir que grande parte do artigo 189.º n.º 1 CPP perdeu campo de aplicação, tendo agora a ingerência no conteúdo do correio eletrónico, mensagens de texto e multimédia, mensagens instantâneas e chamadas realizadas através do sistema *VoiceOverIP* outro regime que não o das escutas telefónicas e regulado em diploma próprio – o que carece de sentido, uma vez que se tratam de meios de obtenção de prova aplicáveis à generalidade dos crimes (com as restrições constantes da "interceção de comunicações" prevista no artigo 18.º da Lei do Cibercrime e as "ações encobertas" previstas no artigo 19.º).

Os métodos de obtenção de prova que contendem com a ingerência no conteúdo das comunicações eletrónicas fechadas dos indivíduos não é, infelizmente, o único ponto da matéria que une Direito e Informática à qual o legislador não tem dado a necessária atenção. Disso é exemplo a falta de sistematização dos tipos materiais de crimes informáticos e relacionados com a utilização da informática, que ora se encontram no Código de Processo Penal, ora na Lei do Cibercrime. Para além deste aspeto é visível a desconsideração do legislador pelas decisões do Tribunal Europeu de Justiça, mantendo em vigor e sem quaisquer reparos leis, cujas soluções foram consideradas como altamente violadoras dos direitos fundamentais dos cidadãos (como é o caso da Lei 32/2008, como visto).

Assim, reclama-se nesta matéria a intervenção do legislador, de modo a evitar confusões concetuais e de institutos processuais, que em tudo prejudicam a hermenêutica jurídica e sistematização, mas acima de tudo que podem constituir grave desconsideração e provável atropelo dos direitos fundamentais dos cidadãos na aplicação do Direito e realização da Justiça.

"Assim haja vontade e imaginação legislativa"[369]

[369] Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59. Página 59.

Bibliografia

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

—. "Notas reflexivas sobre o regime das escutas telefónicas no Código de processo penal português." *O Direito*, 2016 II, ano 148º: 559-583.

Albrecht, Hans-Jörg. "Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos." Em *Que futuro para o direito processual penal?* , de Mário J. Ferreira Monte, 725-743. Coimbra Editora, 2009.

Albuquerque, Paulo Pinto de. *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* 4ª edição. Universidade Católica, 2011.

—. *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem.* Universidade Católica Portuguesa, 2008.

Andrade, Manuel da Costa. *"Bruscamente no verão passado", a reforma do Código de Processo Penal.* Coimbra Editora, 2009.

—. "Nemo tenetur se ipsum accusare e o direito tributário ." *Boletim de Ciências Económicas da Faculdade de Direito da Universidade de Coimbra*, 2014: 385-451.

Andrade, Manuel da Costa. "Métodos ocultos de investigação (pladoyer para uma teoria geral)." Em *"Que futuro para o Direito Processual Penal?" - Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos*, de Mário Ferreira Monte, 525-551. Lisboa: Coimbra Editora, 2009.

Ascensão, José de Oliveira. "A sociedade da informação." Em *Direito da Sociedade da Informação*, de AA VV, 163-184. Coimbra: Coimbra Editora, 1999.

Ascensão, José de Oliveira. *A sociedade digital e o consumidor.* Vol. VIII, em *Direito da Sociedade de Informação,* de AA VV, 123-153. Coimbra: Coimbra Editora, 2009.

Ascensão, José de Oliveira. "Sociedade da informação e liberdade de expressão." Em *Direito*, de AA VV. s.d.

Cabral, José António Henriques dos Santos, e António Jorge Fernandes de Oliveira Mendes. *Notas ao Regime Geral das Contra-Ordenações e Coimas.* Almedina, 2009.

Cabral, José Santos. "Prova Indiciária e as novas formas de criminalidade." *Revista Julgar nº 17*, Maio-Agosto de 2012: 13-33.

Canotilho, Jorge J. Gomes, e Vital Moreira. *Constituição da República Portuguesa anotada, Vol. I.* 4ª edição revista e atualizada. Coimbra Editora, 2007.

Casimiro, Sofia de Vasconcelos. *Mapa da problemática jurídica da Sociedade da Informação.* Vol. IX, em *Direito da Sociedade de Informação*, de AA VV, 31-55. Coimbra Editora, grupo Wolters Kluwer, 2011.

Castro, Catarina Sarmento e. "Protecção de dados pessoais na Internet." *Revista Sub Judice*, Setembro de n.º 35, 2006: 11-29.

Correia, João Conde. "Prova digital: as leis que temos e a lei que devíamos ter." *Revista do Ministério Público n.º 139*, 2014, ano 35: 29-59.

—. "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (artigo 32.º n.º 8 2ª parte CRP)?" *Revista do Ministério Público nº 79*, Julho/Setembro de Ano 20, 1999: 45-67.

Costa, F. Bruto da, e R. Bravo. *Spam e Mail Bomb, Subsídios para uma perspetiva criminal.* Lisboa: Quid Iuris, 2005.

Costa, Joana. "O princípio nemo tenetur na Jurisprudência do Tribunal Europeu dos Direitos do Homem." *Revista do Ministério Público n.º 128*, Outubro-Dezembro de Ano 32, 2011: 117-183.

Costa, José de Faria. "As telecomunicações e a privacidade: o olhar (in)discreto de um penalista." Em *As telecomunicações e o Direito na Sociedade da Informação*, de Instituto Jurídico da Comunicação, 49-78. FDUC, 1999.

—. *Direito Penal da Comunicação. Alguns escritos.* Coimbra Editora, 1998.

Dias, Augusto Silva. "Os criminosos são pessoas? Eficácia e garantia no combate ao crime organizado." Em *Que futuro para o direito processual penal?*, de Mário F. Monte, 687-708. Coimbra Editora, 2009.

—. "O direito à não auto-inculpação no âmbito das contra-ordenações do Código dos Valores Mobiliários." *Revista da Concorrência e Regulação*, Janeiro-Março de Ano 1, 2010: 237-265.

Dias, Figueiredo. *Comentário Conimbricense ao Código Penal, Parte Especial.* Vol. Tomo II. Coimbra Editora, 1999.

—. "Direito Processual Penal - Lições do Prof. Doutor Jorge de Figueiredo Dias, coligidas por Maria João Antunes, Assistente da Faculdade de Direito da Universidade de Coimbra." Coimbra: Secção de Textos da Faculdade de Direito da Universidade de Coimbra, 1998/1999.

Faria, Nuno Serrão. "Acesso aos registos das escutas telefónicas (os poderes de destruição do juiz de instrução)." Em *Prova Criminal e Direito de Defesa*, de Frederico de Lacerda da Costa Pinto Terresa Pizarro Beleza, 201 a 256. Coimbra: Almedina, 2011.

Ferreira, Cavaleiro. *Curso de Processo Penal II.* 1981.

Garcia, Miguez, e Castela Rio. *Código Penal (parte geral e especial) com notas e comentários.* Almedina, 2014.

Gaspar, António Henriques, José António Henriques dos Santos Cabral, Eduardo Maia Costa, António Jorge de Oliveira Mendes, António Pereira Madeira, e António Pires Henriques da Graça. *Código de Processo Penal Comentado.* 1ª. Almedina, 2014.

Gonçalves, Manuel Lopes Maia. *Código Penal Português - Anotado e Comentado - Legislação complementar.* 14. Almedina, 2001.

Jesus, Francisco Marcolino de. *Os meios de obtenção da prova em processo penal.* Coimbra: Almedina, 2015.

Leitão, Adelaide Menezes. *Metatags e o correio eletrónico entre os novos problemas do direito da internet.* Vol. IV, em *Direito da Sociedade da Informação,* de AA VV, 405-432. Coimbra: Coimbra Editora, 2003.

Leite, André Lamas. "Entre Péricles e Sísifo: o novo regime legal das escutas telefónicas." *Revista Portuguesa de Ciência Criminal*, Outubro-Dezembro de 2007, ano 17: 613-679.

Leite, Inês Ferreira. "O novo regime das escutas telefónicas. Uma visão panorâmica sobre a reforma de 2007." Em *Direito da Investigação Criminal e da Prova*, de AA. VV. Almedina, 2014.

Lopes, José Mouraz. "Escutas telefónicas: seis teses e uma conclusão." *Revista do Ministério Público*, Outubro-Dezembro de 2005, ano 26: 139-151.

Loureiro, Flávia Noversa. "A (i)mutabilidade do paradigma processual penal respeitante aos direitos fundamentais em pleno século XXI." Em *Que futuro para o Direito Processual Penal?*, de Mário F. Monte, 269-289. Coimbra Editora, 2009.

Macedo, João Barbosa de. "Algumas considerações acerca dos crimes informáticos em Portugal." Em *Direito Penal hoje, desafios e respostas*, de Manuel da Costa Andrade e Rita Castanheira Neves, 221-262. Coimbra Editora, 2009.

Marques, Garcia, e Lourenço Martins. *Direito da Informática.* Coimbra: Almedina, 2000.

Mata-Mouros, Fátima. "Escutas telefónicas - o que não muda com a reforma." *Revista do CEJ*, 1º semestre de 2008, número 9: 219-242.

Mendes, Paulo de Sousa. "A prova penal e as regras da experiência." Em *Estudos em Homenagem ao Professor Figueiredo Dias, III*, de AA VV, 997-1011. Coimbra Editora, 2010.

Mendes, Paulo de Sousa. "O processo penal entre a eficácia e as garantias." Em *Direito da Investigação Criminal e da Prova*, de AA. VV., 67-80. Almedina, 2014.

Mesquita, Paulo Dá. *Processo Penal, Prova e Sistema Judiciário.* 1ª. Wolkers Kluwer/ Coimbra Editora, 2010.

Miranda, Jorge, e Rui Medeiros. *Constituição Portuguesa Anotada, Tomo I.* 2ª edição. Wolter Kluwer, Coimbra Editora, 2010.

Moniz, Helena. "Internet e Globalização - Problemas jurídico-penais." Em *As telecomunicações e o direito na sociedade da informação*, de Instituto Jurídico da Comunicação, 367-385. Coimbra: Faculdade de Direito da Universidade de Coimbra, 1999.

Monte, Mário Ferreira. "Escutas telefónicas." Em *III Congresso de Processo Penal - Memórias*, de AA. VV., 163-195. Almedina, 2010.

Neves, Rita Castanheira. *As ingerências nas comunicações electónicas em Processo Penal.* 1ª. Coimbra Editora, 2011.

Pereira, J. A. Teles. "O 11 de Setembro e o debate sobre o modelo de Serviços de Informações em Portugal." *Revista do Ministério Público*, Janeiro/Março de 2002, ano 23: 155-164.

Pereira, Joel Timóteo Ramos. *Compêndio Jurídico da Sociedade da Informação.* Lisboa: Quid Iuris, 2004.

Pereira, Patrícia Silva. *Prova Indiciária no âmbito do Processo Penal.* Coimbra: Almedina, 2016.

Pinto, Paulo Mota. "Sobre alguns problemas jurídicos da Internet." Em *As telecomunicações e o direito na sociedade de informação*, de Instituto Jurídico da Comunicação, 350-366. Coimbra: Faculdade de Direito da Universidade de Coimbra, 1999.

Porto, Magistrados do Ministério Público do Distrito do. *Código de Processo Penal, comentários e notas práticas* . Coimbra Editora, 2009.

Ramalho, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital.* Almedina, 2017.

Ramos, Armando Dias. *A prova digital em processo penal: o correio eletrónico.* 2ª. Chiado Editora, 2017.

Ramos, Vânia Costa. "Nemo tenetur se ipsum accusare e concorrência. Jurisprudência do Tribunal de Comércio de Lisboa." *Revista de Concorrência e Regulação n.º 1*, Janeiro-Março de ano 1, 2010: 175-198.

—. "Corpus Iuris 2000 - Imposição ao arguido de entrega de documentos para prova e nemo tenetur se ipsum accusare." *Revista do Ministério Público*, Outubro-Dezembro de 2006, ano 27: 125-149.

Ribeiro, Cristina. "Escutas telefónicas: pontos de discussão e perspetivas de reforma." *Revista do Ministério Público*, Outubro-Dezembro de 2003, ano 24: 67-89.

Rodrigues, Benjamim Silva. *Da prova penal.* Editado por Lda Letras e Conceitos. Vol. Tomo IV. Rei dos Livros, 2011.

—. *Das Escutas Telefónicas, Tomo I, A monotorização dos fluxos informacionais e comunicacioniais.* Coimbra: Coimbra Editora, 2008.

Rodrigues, Cláudio Lima. "Dos pressupostos materiais de autorização de uma escuta telefónica." *verbojuridico.net.* Editado por Verbo Jurídico. Fevereiro de 2013. http://www.verbojuridico.net/ficheiros/doutrina/ppenal/claudiolimarodrigues_autorizacaoescutatelefonica.pdf (acedido em 27 de Dezembro de 2016).

Santos, Cristina Máximo dos. "As novas tecnologias da informação e o sigilo das telecomunicações." *Revista do Ministério Público nº 99*, Julho/Setembro de Ano 25, 2004: 89-116.

Santos, Manuel Simas, Manuel Leal Henriques, e João Simas Santos. *Noções de Processo Penal.* Rei dos Livros, 2010.

Silva, Maria de Fátima Reis. "O direito à não auto-incriminação." *Sub Judice n.º 40*, 2007: 59-74.

Silva, Sandra Oliveira e. "O arguido como meio de prova contra si mesmo: considerações em torno do princípio nemo tenetur se ipsum accusare." *Revista da Faculdade de Direito da Universidade do Porto,* Ano X, 2013: 361-379.

—. "Legalidade da prova e provas proibidas." *Revista Portuguesa de Ciência Criminal*, 2011, ano 21, número 4: 545-591.

Valente, Manuel. *Conhecimentos fortuitos. A busca de um equilíbrio apuleiano.* Coimbra: Almedina, 2006.

Venâncio, Pedro. *Lei do Cibercrime - Anotada e Comentada.* Wolters Kluwer Portugal, Coimbra Editora, 2011.