Universidade Católica Portuguesa, Centro Regional do Porto
Faculdade de Direito – Escola do Porto

OS MEIOS DE OBTENÇÃO DE PROVA NO AMBIENTE DIGITAL: O CORREIO ELECTRÓNICO

Dissertação de Mestrado na área de Direito Criminal apresentada à Universidade Católica Portuguesa, por Vera L. Azevedo Monteiro, sob orientação do Professor Doutor José Manuel Damião da Cunha.

UNIVERSIDADE CATÓLICA PORTUGUESA

PORTO
2016

Universidade Católica Portuguesa, Centro Regional do Porto
Faculdade de Direito – Escola do Porto

OS MEIOS DE OBTENÇÃO DE PROVA NO AMBIENTE DIGITAL: O CORREIO ELECTRÓNICO

Dissertação de Mestrado na área de Direito Criminal apresentada à Universidade Católica Portuguesa, por Vera L. Azevedo Monteiro, sob orientação do Professor Doutor José Manuel Damião da Cunha.

PORTO
2016

Agradecimentos

Ao longo do meu percurso académico, que culminou com a redação da tese de mestrado, foram várias as pessoas que me encorajaram e me acompanharam para alcançar esta meta.

Primeiramente, gostaria de expressar o meu profundo agradecimento ao Senhor Professor Doutor José Manuel Damião da Cunha, por toda a orientação, partilha de conhecimentos e disponibilidade.

Dirijo, igualmente, um agradecimento a toda a equipa de *CSPP PSA Services Portugal*, pela compreensão que sempre demonstraram face às necessidades de tempo que teve que ser despendido a favor desta investigação.

Por último, mas não menos importante, à minha família, em especial à minha avó, aos meus amigos e aos meus colegas que me incentivaram a percorrer este caminho e que foram sempre uma presença constante e incansável ao longo do meu percurso.

Introdução

A *Internet* e as tecnologias de informação e comunicação revolucionaram o mundo como hoje o conhecemos, e obviamente o Direito não ficou indiferente a esta mudança.

Com o surgimento destes novos meios de comunicação surgiram também um novo tipo de criminalidade, o cibercrime ou criminalidade informática, assim por forma a dar resposta a futuros comportamentos desviantes foi essencial a previsão legislativa desta questão.

Por criminalidade informática podemos entender como o conjunto de comportamentos desviantes perpetrados através de um sistema informático ou contra um sistema informático.

Apesar de ser uma realidade recente, o legislador já mostrava preocupação para responder a esta nova criminalidade. A primeira legislação a surgir sobre esta temática foi a Lei n.º 109/91, de 17 de Agosto ou "Lei da Criminalidade Informática", posteriormente revogada pela Lei 109/2009, de 15 de Setembro a Lei do Cibercrime.

No entanto, a lacuna da Lei da Criminalidade Informática, só é colmatada em 2001 com a Convenção de Budapeste, intitulada de Convenção do Cibercrime, esta Convenção previu os primeiros mecanismos processuais para a prova em formato digital ainda assim, só em 2009 foi contemplado no nosso ordenamento jurídico a previsão destes instrumentos processuais que permitissem não só a apreensão, mas também a investigação da criminalidade informática.

O que se pretendeu com esta legislação não foi apenas a tipificação legal das condutas criminosas, mas também a regulamentação da prova digital uma vez que anteriormente a 2009, a prova em suporte eletrónico regia-se pelo regime das escutas telefónicas previsto no art.º 189º do Código de Processo Penal e consequentemente, aos requisitos previstos no art.º 187ºdo CPP

A revisão do Código de Processo Penal em 2007 e a subsequente adoção das iniciativas internacionais culminaram com a adoção da Lei nº. 32/2008 e a Lei nº. 109/2009, o legislador deixou em aberto várias questões quanto à articulação entre estes diplomas, nomeadamente, como se articulam as normas entre si? Existe uma revogação do regime geral?

O regime previsto para a prova digital encontra-se atualmente fragmentado e lacunoso, originando zonas cinzentas que suscitam uma aplicação incoerente. Seria de esperar que as lacunas até então fossem colmatadas, ao invés o legislador acentuou a incoerência e assimetria na regulamentação desta matéria.

O que pretendemos com esta dissertação é analisar o regime para este meio de prova, sempre com um espírito crítico, de forma a alcançar respostas para as questões suscitadas pelas reformas legislativas, focando-nos não só no correio eletrónico, mas também nos meios de registo comunicacionais equiparáveis.

Correio Eletrónico enquanto prova digital

1. Considerações gerais e a conceptualização do correio eletrónico enquanto meio comunicacional.

Com o advento das novas tecnologias, o direito enfrenta novos desafios, desde logo com o surgimento de novas formas de comunicação, passamos da rudimentar carta como correspondência, para o fax, o correio eletrónico, as SMS entre outros meios que são cada vez mais utilizados, não só porque são meios menos dispendiosos, mas também porque são mais expeditos e encontram-se à distância de apenas um clique.

Com o surgimento destas novas formas de comunicação houve uma necessidade de adaptação do Direito às novas realidades informacionais e comunicacionais, de forma a poder responder aos novos desafios, a identificar o surgimento de condutas desviantes também no mundo digital e a sancionar os respetivos comportamentos criminosos, isto por força do princípio da necessidade, postulado no art.º 18º nº 2 da Constituição da República Portuguesa.

Desta feita, e tendo em conta que nos iremos centrar essencialmente no correio eletrónico, foi necessário delimitar uma política de atuação para responder a uma nova realidade criminosa, a criminalidade informática.

Assim no seio da União Europeia, como resposta a esta realidade, podemos destacar a Diretiva nº 2002/58/CE[1], neste diploma o legislador europeu, procurou definir um conceito de correio eletrónico no seu art.º 2º alínea h) como "*qualquer mensagem textual, vocal, sonora ou gráfica enviada através de a rede pública de comunicações de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário as recolher"*.

Na transposição desta mesma diretiva não foi adotado este conceito de correio eletrónico no nosso ordenamento jurídico nacional. Desta feita, dada a insuficiência[2] desta definição, vários autores avançaram com uma definição própria de correio eletrónico enquanto meio de correspondência, entre estes destacamos ARMANDO VEIGA e BENJAMIM SILVA RODRIGUES que definem o correio eletrónico como *"sendo um fluxo informacional e comunicacional digital, sob o formato de texto, voz, som, informacional e comunicacional (tendencialmente) fechado, através de um ponto terminal da rede, na rede pública de comunicações eletrónicas, conduzida até ao servidor*

[1] A Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

[2] De acordo com ARMANDO DIAS RIBEIRO, o legislador europeu ficou muito aquém pois "não se socorreu da imagem da correspondência tradicional para definir correio eletrónico, nem tão-pouco lhe atribuiu qualquer conotação com a correspondência tradicional", ARMANDO DIAS RAMOS, "*A prova digital em Processo Penal: o correio eletrónico"*, Chiado Editora, 1ª edição, Novembro de 2014.

de mail ou ao terminal do destinatário de fluxo até que o mesmo proceda à sua recolha, leitura e/ou posterior eliminação"[3].

Já, ROMEO CASABONA, define correio eletrónico como *"uma modalidade de comunicação, em geral de carácter pessoal, que incorpora texto, som e imagem e que se serve das redes telemáticas como tecnologia de transmissão e dos sistemas informáticos (computadores e o software ou sistema lógico corresponde) como instrumentos de emissão e receção entre dois ou mais comunicantes e nesse caso de armazenamento de mensagens"*[4].

Por outro lado, ARMANDO DIAS RAMOS, discorda com as definições apresentadas por estes autores, entende que o conceito não foi bem realizado[5], por isso sugere como conceito de correio eletrónico o seguinte: "*programa informático que permite a comunicação instantânea, de modo diferido, entre quem a envia e quem a recebe, através das redes de informação e comunicação, independentemente do local em que estes se encontrem, sem a necessidade deste se encontrar instalado no computador (…) Assim, pode concluir-se que o correio eletrónico detém as seguintes características indissociáveis: é eletrónico, assíncrono, ubíquo, digital e informático (…)".*[6]

Assim dada à inegável realidade que o correio eletrónico constitui atualmente entre nós um novo meio de comunicação expedito e que acarreta poucos custos, não é de surpreender que a maioria das pessoas possuam e utilizem este meio de comunicação diariamente.

Tratando-se de um meio de comunicação que permite uma comunicação à distância de forma célere, segura e mais sofisticada que outros meios existentes até então, não é de admirar que, atualmente, muita da atividade criminosa, utilize estes tipos de meios quer para comunicar quer para atuar.

Verificamos, por isso, uma modificação do *modus operandi*, já que se trata de um meio expedito, é compreensível que a atividade criminosa faça uso deste tipo de meios para comunicar ou até mesmo manter a sua atividade criminosa (ex.: instalação de vírus que permitam o acesso às contas bancárias, a contas de email, a vigilância da atividade informática do utilizador[7]).

---

[3] ARMANDO VEIGA e BENJAMIM SILVA RODRIGUES, *"Escutas telefónicas, rumo à monitorização dos fluxos informacionais e comunicacionais digitais"*, Coimbra Editora, 2ª Edição, 2007.

[4] CARLOS MARIA ROMEO CASABONA, *"La protección penal de los mensajes de correo electrónico y de otras comunicaciones de catácter personal a través de internet" ob.cit.* pág. 129, artigo acessível online através https://www.unifr.ch/ddp1/derechopenal/obrasportales/op_20080612_17.pdf

[5] *"(…) ao escrever-se um endereço no browser da internet, está a enviar-se a informação desse endereço a um servidor alojado na Internet e, por sua vez, a receber-se a comunicação do carregamento dessa página Web".* ARMANDO DIAS RAMOS, "A prova digital em Processo Penal: o correio eletrónico", Chiado Editora, 1ª edição, Novembro de 2014.

[6] ARMANDO DIAS RAMOS, *"A prova digital em Processo Penal: o correio eletrónico",* (…) *ob.cit.* pág. 11.

[7] Como por exemplo, o típico cavalo de Tróia que se infiltram no computador do utilizador com o intuito de recolha de informação, outro caso semelhante são os sites de *phishing*, podemos ainda destacar os *keyloggers* que são programas informáticos que permite a memorização, em tempo real, todas as teclas pressionadas, sem o conhecimento da vitima de forma a obter dados sensíveis que são posteriormente enviados, e por último, temos o caso dos *ransomware* tratam-se de vírus que restringem o acesso ao sistema infetado, por exemplo a um conjunto de ficheiros que se encontram no computador do utilizador, e cobra um valor de "resgate", maioritariamente monetário, para que o acesso possa ser reestabelecido.

Desta forma, há muito que havia necessidade de se responder legalmente ao surgimento desta a nova realidade criminal e foi após sucessivas revisões ao Código de Processo Penal, que chegamos ao regime hoje previsto no art.º 189º do CPP.

2. O Código de Processo Penal e a reforma da era digital.

O atual Código de Processo Penal tem a sua origem no Decreto Lei nº 78/87, de 17 de Fevereiro, contudo este diploma sofreu várias reformas, a última revisão data de 2016 e constitui a vigésima quinta alteração ao diploma original.

Tendo em conta a temática que nos ocupa, iremos apenas abordar as reformas que conduziram ao atual regime do correio eletrónico e a respetiva equiparação ao regime das escutas telefónicas de forma a poder fazer uma contextualização da presente regulamentação.

Na sua versão original o Código de Processo Penal de 1987, previa no Título de "meios de obtenção de obtenção de prova", Capitulo IV "Das escutas telefónicas", o art.º 190º, que consagra também uma extensão do regime das escutas telefónicas para as "conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone."

Daqui podemos desde já concluir que esta norma não foi das mais felizes, pois suscita várias incertezas e dúvidas interpretativas, por exemplo esta equiparação valeria apenas para a palavra falada ou também para outros meios de comunicação como os escritos? O legislador não foi claro.

Pelas diversas questões interpretativas suscitadas, em 1998 procedeu-se à nona alteração ao Código de Processo Penal através da Lei nº 59/98, de 25 de Agosto, com esta reforma o art.º 190º sofreu uma significativa alteração passando a dispor que *" O disposto nos artigos 187.º, 188.º e 189.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, bem como à interceção das comunicações entre presentes."*.

Com esta alteração, ficou claro que o correio eletrónico estava no âmbito da extensão do regime das escutas telefónicas contudo, com a Lei nº 48/2007, de 29 de Agosto, o regime previsto para as escutas sofreu grandes alterações. O art.º 190º passou a prever o efeito de nulidade, passando o art.º 189º a consagrar a extensão do regime das escutas telefónicas a outras formas de comunicação.

De acordo com RITA CASTANHEIRA NEVES, esta alteração acabou por colocar um "ponto final" em algumas divergências na doutrina e na jurisprudência nacional, como por exemplo relativamente *"ao círculo de pessoas sujeitas a escutas, suas limitações temporais, aos requisitos de destruição de prova e ao papel do juiz no controlo da legalidade"*[8]. Partilhamos da mesma opinião contudo, a solução escolhida pelo legislador para o correio eletrónico ao remeter para o regime das escutas telefónicas foi imprudente, talvez por desconhecimento das especificidades do meio de comunicação em causa.

[8] RITA CASTANHEIRA NEVES, *"As ingerências nas Comunicações eletrónicas em Processo Penal"*, Coimbra editora, 2011, *ob.cit.* pág. 140.

Relativamente, às alterações sofridas pelo art.º 189º que passa a incorporar a extensão do regime das escutas telefónicas, o anterior art.º 190º passou a consagrar, no seu nº 1 o seguinte: "*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.",* e por outro lado, foi acrescentado um nº2, passando este a dispor 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.",* no fundo consagra, expressamente a possibilidade de registo de dados obtidos através da localização celular, assim como dispõe sobre o seu âmbito e admissibilidade.

Traçado o percurso legislativo, o correio eletrónico assume-se, hoje em dia, como uma ferramenta essencial para comunicação e inclusive um instrumento de trabalho para grande parte das pessoas.

O surgimento da *Internet* veio revolucionar o mundo como até então era conhecido e o direito não ficou aquém, evoluiu e respondeu aos desafios propostos pela nova era digital que hoje vivemos, consagraram-se novos crimes, como os crimes praticados através de um sistema informático, e consequentemente novos meios de obtenção de prova[9] a par das buscas e das apreensões.

Posto isto, iremos proceder a uma análise do regime previsto no Código de Processo Penal para o correio eletrónico, com o intuito de esclarecer algumas questões que se levantam a uma primeira vista, nomeadamente, se existe um verdadeiro paralelismo entre as escutas telefónicas e o correio eletrónico. Tratando-se de uma comunicação, quando finda esse processo? Quando chega à caixa de correio ou quando já se encontra lido? Findo o processo de comunicação estaremos no âmbito da tradicional correspondência previsto no art.º 179º CPP? Estas são algumas das questões que pretendemos ver respondidas.

[9] É inegável que o correio eletrónico constitui um meio de prova admissível de acordo com o art.º 125º do Código de Processo Penal, que prevê o princípio da admissibilidade de prova. As provas em suporte eletrónico são admissíveis em tribunal, desde que obtidas de acordo com um critério de legalidade.

ARMANDO DIAS RAMOS, propõe uma definição de prova digital, visto que o legislador não positivou a definição da mesma na Lei 109/2009, vulgo Lei do Cibercrime, este autor propõe o seguinte sentido para a prova em suporte informático *"toda a informação passível de ser obtida ou extraída de um dispositivo eletrónico (local*, *virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital para além de ser admissível, precisa e completa.", cfr.* ARMANDO DIAS RAMOS, "*A prova digital em Processo Penal: o correio eletrónico"*, (…) *ob.cit.* pág. 44.

Dada a novidade deste tipo de prova, e face à carência legislativa no nosso ordenamento jurídico, foram apresentadas duas propostas sobre a prova digital, o Projeto de lei nº 208/IX "Garante a proteção dos dados pessoais e a privacidade das comunicações eletrónicas na sociedade de informação, procedendo à transposição da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2012" e o Projeto de Lei nº 217/IX que debruçava-se sobre a temática do "Regime Jurídico da obtenção de prova digital eletrónica na Internet", contudo nenhum dos diplomas entrou em vigor, no entanto esta iniciativa de positivação da prova digital, serviu de inspiração para a origem da Lei nº 32/2008, de 17 de Julho, relativa à conservação de dados gerados ou tratados n contexto da oferta de serviços de comunicações eletrónicas.

3. Repercussões de uma Reforma irrefletida, equiparação do correio eletrónico ao regime das escutas telefónicas.

3.1. Crítica doutrinal:

Com o ímpeto tecnológico o legislador teve que responder a estes novos desafios, os crimes passaram a ser cometidos através de um computador e de redes de comunicações eletrónicas, assim foi necessária uma atuação de forma a responder a esta nova criminalidade, através de uma repressão e prevenção, eram estes os principais objetivos da Revisão de 2007.

Contudo, esta foi encarada por grande parte da doutrina, como uma oportunidade perdida de mudança de paradigma normativo e de dar resposta às mudanças fruto desta era tecnológica. De acordo com MANUEL DA COSTA ANDRADE, esta reforma deveria ter "*substituído o capitulo das escutas telefónicas por outro mais amplo e compreensivo, contendo um regime geral e comum às diferentes formas de intromissão nas telecomunicações"*[10] .

Estamos de acordo com este autor, esta reforma em vez de responder às questões, gerou ainda mais dúvidas interpretativas, tais como, aplicando-se um regime jurídico que tem por objeto uma comunicação eletrónica quando é que sabemos no caso, do correio eletrónico, quando é que finda esse processo comunicacional? Existem vários momentos? Qual o regime previsto para cada um deles?

Estando perante uma área que visa a proteção do sigilo das comunicações o que se pretende acautelar são as intromissões nas comunicações por terceiros, por isso para fazermos uma cuidada análise do regime atual para o correio eletrónico devemos ter também em conta o particular processamento da comunicação.

Fruto da crescente cibercriminalidade, a ingerência nas comunicações é uma realidade cada vez mais presente nas investigações criminais, mas sempre tendo em conta os limites impostos constitucionalmente que visam a salvaguarda da privacidade e da inviolabilidade das comunicações.[11]

Com a extensão do regime das escutas telefónicas ao correio eletrónico, surgiram na doutrina várias vozes dissonantes quanto ao tratamento e processamento deste meio de comunicação, sobretudo quando este chega ao seu destinatário e se encontra armazenado no computador.

Assim, o regime das escutas telefónicas abrange qualquer mensagem enviada através de uma rede pública de comunicações, que poderá ser armazenada na rede ou no computador do utilizador, mesmo que "guardada em suporte digital". Isto significa que o processo de comunicação finda quando o correio eletrónico chega ao seu destinatário ou quando já foi lido pelo destinatário?

---

[10] MANUEL DAS COSTA ANDRADE, "Bruscamente no Verão passado; a Reforma do Código de Processo Penal, observações criticas de uma lei que podia e devia ter sido diferente", Coimbra Editora 2009 *ob.cit.* pág. 184 a 187.

[11] *Cfr.* art.º 34 nº4 da Constituição da República Portuguesa.

De acordo com o entendimento de MANUEL DA COSTA ANDRADE[12], quando o *e-mail* já foi recebido, lido e armazenado no computador, deixa automaticamente de integrar o conceito de telecomunicação, passando a valer como mero "escrito", deixando de ter proteção do regime previsto no art.º 189º[13].

Este autor vai ainda mais longe, entende que a partir do momento que há *"entrada dos dados ou noticias na esfera de domínio do destinatário, este deixa de estar naquela especifica situação de perigo e de carência de tutela"* e como tal, a comunicação deixa de estar exposta a uma heteronomia por parte do fornecedor do serviço, podendo o destinatário munir-se de meios de tutela para evitar ingerências indesejadas de terceiros. Contudo MANUEL DA COSTA ANDRADE faz a ressalva de que *"não deve identificar-se o fim do processo dinâmico de transmissão com a sua chegada ao (último) aparelho (...) do destinatário, (...) também aí pode revelar-se e atualizar-se a posição de domínio do sistema de telecomunicação. Que pode continuar a intrometer-se arbitrariamente no conteúdo e nos dados da comunicação à margem do controlo do(s) interlocutor(es)".*

Noutro sentido, PEDRO VERDELHO[14] defendeu, mesmo antes da reforma de 2007, um regime tripartido do acesso em investigação. Este autor, assume que a "vida" do correio eletrónico é constituída por três momentos, e a cada momento corresponde um regime distinto.

Primeiramente, o *email*, enquanto se encontra em transação poderá ser alvo de uma interceção em tempo real, neste momento deve ser submetido ao regime das escutas telefónicas, uma vez que estamos perante uma verdadeira comunicação eletrónica. Por outro lado, quando o *email* chega ao domínio do destinatário, e apesar de não se encontrar lido, a comunicação cessa e o correio eletrónico assume agora a forma de ficheiro digital assim, deverá ser remetido para o regime da apreensão de correspondência previsto no art.º 179º do CPP.

Finalmente, se o *email* já foi aberto e lido, trata-se de um ficheiro em formato digital e como tal o meio de obtenção de prova deverá ser o regime das apreensões previsto no Capítulo III (Das apreensões), do Título III (Dos meios de obtenção de prova) do Código de Processo Penal[15].

Não nos parece que seja razoável a existência de três regimes distintos para uma mesma realidade, na verdade em termos de investigação criminal seria um caos processual. Como é que iriamos saber se o *email* já tinha ou não sido lido porque atualmente qualquer ferramenta de correio eletrónico permite, após a visualização do seu conteúdo, "marcar como não lido".

Já RITA CASTANHEIRA NEVES, discorda com a existência desta posição intermediária assumida por PEDRO VERDELHO, para esta autora o correio eletrónico

---

[12] MANUEL DAS COSTA ANDRADE, "*Bruscamente no Verão passado; a Reforma do Código de Processo Penal, observações criticas de uma lei que podia e devia ter sido diferente*", (…) *ob.cit.* pág. 156 a 160.

[13] Encontrando-se o *email,* recibo, lido e armazenado, de acordo com este autor este deve ser sujeito *"ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado. Podendo, como tal, figurar como objeto idóneo da busca, em sentido tradicional."*. Esta busca pauta-se pela apreensão do computador ou então através de uma cópia do conteúdo do mesmo.

[14] PEDRO VERDELHO, "*Apreensão de Correio Eletrónico em Processo Penal*", in Revista do Ministério Público, Ano 25.º, 2004, *ob.cit.* pág. 153 e ss.

[15] Antes da reforma de 2007, havia alguma jurisprudência que seguia esta visão tripartida, *cfr*. Acórdão do Tribunal da Relação de Lisboa, de 15 de Julho de 2008, consultável em: http://www.dgsi.pt/jtrl.nsf/0/9182245992c7c5d180257490005 03b8c?OpenDocument

que já chegou ao seu destino mas ainda não foi lido, *"continua com o seu status de comunicação eletrónica não havendo razão para a diferenciação de regime estabelecida quanto ao estado anterior, em que a comunicação eletrónica transitava em rede entre o ponto emissor e recetor devendo ser aplicado também neste momento de espera o regime de interceção de comunicações eletrónicas"*[16].

Concordamos com a posição de RITA CASTANHEIRA NEVES e em parte com a posição defendia por MANUEL DA COSTA ANDRADE, o correio eletrónico depois de alcançar a esfera do domínio do destinatário, vulgo a sua "caixa de entrada", continua a estar sujeito ao regime de ingerência nas comunicações até este ser lido e aberto, pois até lá as entidades fornecedoras de serviço ainda detêm uma posição de domínio, e só após esse momento é que deixamos de estar perante uma comunicação, não sujeita à especial tutela do sigilo das comunicações (art.º 189º CPP), mas sim ao regime previsto para a correspondência. Porém, iremos posteriormente adensar mais esta perspetiva.

Esta visão tripartida do correio eletrónico foi, atualmente, ultrapassada com a Revisão de 2007, o correio que se encontre armazenado em formato digital é, de acordo com o art.º 189º, remetido para o regime das escutas telefónicas.

Outro autor que manifestou a sua posição face a esta extensão, foi BENJAMIM SILVA RODRIGUES[17], este autor segue a "*posição de fidelidade ao regime de paradigma de ponderação constitucional e legalmente codificado em matéria de intervenções telefónicas"*, quer isto dizer que, a equiparação do correio eletrónico ao regime das escutas telefónicas constitui uma desvirtuação ao paradigma constitucional previsto para as escutas, que foi pensada exclusivamente para palavras "faladas" e não escritas.

Porém, se fizermos uma interpretação atualista sem ter em conta o paradigma originário da codificação podemos admitir a monitorização deste tipo de comunicações.

Assim, a vida do *email* teria também três momentos iguais aos mencionados *supra.* Relativamente ao primeiro momento (monitorização em tempo real), estaríamos perante uma comunicação eletrónica, que se encontra em trânsito e como tal poderia aplicar-se o regime das escutas telefónicas, procedendo-se a uma clonagem da mensagem em trânsito e consequente desvio do mesmo; quanto ao segundo momento (monitorização das comunicações eletrónicas que se encontram armazenadas na rede ou no equipamento, pendentes ainda de serem lidas pelo destinatário) aqui, apesar da mensagem ter chegado ao seu destino e esta ainda se encontrar por ler, o autor entende que se deverá aplicar na mesma o regime previsto para as escutas telefónicas, visto que ainda se trata de uma comunicação eletrónica; por último, o terceiro momento (a mensagem foi recebida e lida pelo seu destinatário), o autor considera que não estamos perante um documento eletrónico, mas sim perante um documento que contém "*dados de carácter pessoal no contexto das redes e serviços das comunicações eletrónicas acessíveis ao público"* desta feita, defende que deverá ter-se em conta o disposto na Lei nº 41/2004, de 18 de Agosto (Lei de Proteção da Privacidade e no Sector das Comunicações Eletrónicas) e a Lei 67/98, de 26 de Outubro (Lei de Proteção de Dados Pessoais).

[16]RITA CASTANHEIRA NEVES, "As ingerências nas Comunicações eletrónicas em Processo Penal", Coimbra editora, 2011, *ob.cit.* pág. 149 e ss.

[17] BENJAMIM SILVA RODRIGUES, "das escutas telefónicas - A monitorização dos fluxos informacionais e comunicacionais, Tomo I", Coimbra Editora, 2008, *ob.cit.* pág. 455 e ss.

Na senda da crítica doutrinária, destacamos ainda CARLOS ADÉRITO TEIXEIRA, pronunciou-se no mesmo sentido de que as mensagens eletrónicas recebidas e impressas não estão contempladas pelo regime das escutas telefónicas[18].

Posto isto, e expostas a posições de grande parte da doutrina relativamente ao atual regime, é do nosso entendimento que a Reforma de 2007 não foi a mais feliz, ao invés de responder à altura aos desafios propostos, decidiu "varrer a questão para debaixo do tapete" e fazer uma extensão a um regime que suscita ainda mais questões, por isso tentaremos, de seguida, esclarecer.

3.2. Deveria o correio eletrónico ser reconduzido ao regime das escutas telefónicas?

Expostas as principias posições doutrinais, cabe-nos agora tecer a nossa posição face à tomada de posição do legislador quando remete o correio eletrónico e outros meios de comunicação para o regime das escutas.

Dada a génese do paradigma da norma que prevê o regime das escutas telefónicas e na senda do pensamento defendido por BENJAMIM SILVA RODRIGUES[19], concordamos que o regime das escutas telefónicas, previsto no Código de Processo Penal, dirige-se sobretudo à proteção da palavra falada e não à proteção da palavra escrita.

O regime das escutas foi previsto para a interceção de conversas telefónicas e com isto não queremos dizer que este regime não será o mais adequado porque o meio previsto inicialmente para estas conversações seria o telefone e o meio utilizado pelo correio eletrónico é a *Internet*[20]*,* o que está aqui em causa é a proteção da palavra falada, que a meu ver a sua interceção constitui uma medida mais gravosa e intrusiva para a privacidade da vida privada e para a inviolabilidade das comunicações.

Por outro lado, dada a intromissão que constitui a ingerência numa conversação telefónica, é compreensível que a sua admissibilidade esteja sujeita a um catálogo de crimes mais estrito (art.º 187º nº1 CPP), no entanto, para o correio eletrónico o catálogo de crimes previsto, e partilhando a opinião de RITA CASTANHEIRA NEVES, não deveria ser tão restritivo, somente dessa forma poderíamos dar resposta a criminalidade punível com pena de prisão inferior a 3 anos (cfr. Art.º 187º nº 1 a) CPP), poderíamos também prever a punição de crimes e injúria, de ameaça, de coação e da devassa da vida privada, uma vez que o atual regime prevê apena a sua punição quando o meio utilizado para a prática do crime é o telefone (art.º 187º nº1 al. e) CPP).

Por último, e não querendo entrar por conceitos técnicos, o art.º 189º prevê a extensão do regime das escutas telefónicas ao correio eletrónico mesmo que este se encontre "guardado em formato digital".

---

[18] CARLOS ADÉRITO TEIXEIRA, Revista do CEJ (nº9), 1º semestre 2008, *ob.cit.* pág. 283

[19] BENJAMIM SILVA RODRIGUES, "*Das escutas telefónicas - A monitorização dos fluxos informacionais e comunicacionais, Tomo I*", Coimbra Editora, 2008, *ob.cit.* pág. 455 e ss.

[20] Por exemplo se a for utilizada a *internet* para a realização de uma chamada telefónica, através de *Whatsapp, Skype, Facebook,* somos do entendimento que estamos perante uma comunicação eletrónica e como tal subsumível ao regime das escutas telefónicas.

Ora, as ingerências nas comunicações, por exemplo telefónicas, ocorrem em tempo real, isto também poderá acontecer com o correio eletrónico e as SMS quando estas se encontrem em trânsito.

No entanto, como se processa esta ingerência quando a mensagem chega ao domínio do seu destinatário e já estiver lida?

De acordo com RITA CASTANHEIRA NEVES, não é possível uma interceção pois, *"chegada ao seu destino final e depois de aberta e lida, a mensagem de correio eletrónico já não é nenhuma telecomunicação, ela é já apenas um suporte informático. Já não está em transito. Já não é passível de ser intercetada"*[21].

Posto isto, não entendemos o porquê do legislador submeter ao regime das escutas telefónicas um ficheiro que por si só já não constitui uma comunicação.

Desta forma, não haverá uma ingerência propriamente dita o que poderá ocorrer será uma busca ou gravação do documento.

Em suma, é do nosso entendimento que o legislador podia e devia ter feito uma separação do regime das escutas telefónicas, com isto não queremos dizer que somos apologistas da teoria da equiparação do correio eletrónico à correspondência tradicional[22]l, pelo contrário, entendemos que o correio eletrónico tal como as SMS deveria ter uma previsão autónoma e consequentemente deverá ser feita uma revisão ao Código de Processo Penal. Somente desta forma, é possível dar resposta aos atuais desafios impostos por esta era digital, através da prevenção e repressão de comportamentos desviantes perpetrados através de um meio informático.

Na senda deste pensamento de autonomização surge a lei 109/2009 de 15 de Setembro relativa à Cibercriminalidade e a Lei 32/2008 de 17 de Julho, sobre as quais nos iremos ocupar nos próximos capítulos.

---

[21] Cfr. RITA CASTANHEIRA NEVES, "As ingerências nas Comunicações eletrónicas em Processo Penal", Coimbra editora, 2011, *ob.cit.* pág. 182 e ss.

[22] De acordo com esta posição o correio eletrónico, quando atinge a esfera de domínio do destinatário é equiparável ao regime previsto para o correio tradicional, ou seja, o correio eletrónico traduz-se numa alternativa à carta tradicional pois o que está em causa é a correspondência e não as telecomunicações.

Desta feita, o regime subsumível para a sua apreensão seria o previsto no art.º 179º do CPP, segundo este artigo (nº1), a apreensão da correspondência ocorre com autorização por despacho judicial relativamente a 1) correspondência expedida pelo suspeito a é a ele dirigida; 2) quando está em causa um crime punível com pena de prisão superior a três anos; e 3) quando esta se revelará de grande interesse para a descoberta da verdade ou para a prova.

No nº 2 desta norma, o legislador prevê a proibição do controlo da correspondência entre o arguido e o seu defensor.

Para além disto, no nº 3 encontra-se plasmada a obrigação de que após a apreensão a primeira pessoa a ter conhecimento do seu conteúdo será o juiz que proferiu o despacho.

Posto isto, de acordo com este regime, a apreensão do correio eletrónico estaria sujeita a apertados critérios, como os expostos no nº 3.

Contudo, não nos parece que esta seja a melhor interpretação deste meio de comunicação, nesta senda RITA CASTANHEIRA NEVES afirma que o correio eletrónico *"(...) apenas por ser uma forma de correspondência, se deva reconduzir automaticamente ao regime estabelecido para a correspondência dita tradicional. O correio eletrónico não utiliza as redes postais publicas para a sua transmissão, mas sim as redes e os serviços de comunicações eletrónicas acessíveis ao publico."*.

Contudo, esta teoria já se encontra ultrapassada, uma vez que o legislador assumiu uma posição em contrário, subsumindo ao regime das escutas telefónicas.

4. A atual autonomização, a lei 32/2008 e a lei 109/2009.

4.1. Considerações gerais

A prova digital, para além de se encontrar regulada no Código de Processo Penal (art.º 189º), como vimos anteriormente, encontra-se também prevista na Lei nº 32/2008, de 17 de Julho (relativamente à conservação de dados gerados ou tratados no âmbito da oferta que temos pelos serviços de comunicações eletrónicas) e na Lei do Cibercrime (Lei nº 109/2009, de 15 de Setembro).

A regulação desta matéria constitui atualmente uma manta de retalhos, visto que a mesma matéria se encontra regulada por três diplomas distintos originando uma maior dissimetria e incoerência no nosso ordenamento jurídico, *"esta trilogia para além de acentuar o atual paradigma de descodificação e de negar a desejável centralidade normativa do Código de Processo Penal, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático."* [23]

Posteriormente à entrada em vigor da revisão do Código de Processo Penal, foi necessário um processo de transposição de compromissos internacionais, que culminaram com o surgimento dos dois diplomas mencionados anteriormente, aos quais iremos analisar nos seus aspetos mais essenciais.

4.2. A legislação que temos

4.2.1. LEI 32/2008, de 17 de Julho:

Relativamente à Lei nº 32/2008, de 17 de Julho (transposição da Diretiva nº 2006/24/CE do Parlamento Europeu e do Conselho de 15 de Março), diz respeito à conservação de dados gerados ou tratados, isto é, regula a conservação e transmissão dos ditos dados de tráfego, localização e dados que permitam identificar o utilizador do serviço quando perante uma investigação, deteção ou repressão de crimes graves por parte das autoridades competentes (art.º 3 nº 1).

Contudo, a transmissão dos dados quer de tráfego e localização, quer de dados que permitam a identificação dos utilizadores só será admissível mediante despacho fundamentado pelo juiz de instrução, quando se revele que esta diligência seja indispensável para a descoberta da verdade ou para a prova que de outra forma seria impossível de ou muito difícil de obter de outra forma (art.º 9 nº 1), sem nunca esquecer os princípios de necessidade, proporcionalidade e adequação (art.º 9 nº 4).

Refere ainda que os dados deverão ser conservados por um período máximo de um ano (art.º 6º) e que os dados transmitidos só poderão ser relativos ao suspeito ou arguido, a pessoa que sirva de intermediário, relativamente à qual haja fundadas razões

[23] JOÃO CONDE CORREIA, *"Prova digital: as leis que temos e a lei que devíamos ter"*, Revista do Ministério Público 139: Julho: Setembro 2014

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 (art.º 9º nº 3).

Posteriormente, caso os dados deixem de ser estritamente necessários para a investigação, o juiz determina, oficiosamente ou a requerimento de interessados, a respetiva destruição dos mesmos (art.º 10º nº 1 e nº 2).

Posto isto, e na senda de JOÃO CONDE CORREIA, partilhamos a opinião de que *"o legislador sem qualquer razão técnica válida, duplicou os regimes, consagrando normas gerais no Código de Processo Penal e normas especiais na lei nº 32/2008"*[24].

De facto, não vemos qualquer impedimento para que as questões mais específicas fossem reservadas a esta diploma, contudo esta regularização poderia ter sido, em parte, prevista no Código de Processo Penal, de forma a evitarmos a atual descentralização normativa relativamente à matéria da prova digital.

4.2.2. LEI Nº 109/2009, de 15 de Setembro:

O Estado Português assinou, a 23 de Novembro de 2001, a Convenção de Budapeste sobre o Cibercrime, neste diploma encontrava-se já previsto um completo regime processual que impunha a respetiva transposição para o ordenamento jurídico interno.

Contudo, só a 15 de Dezembro de 2009 esta Convenção é aprovada pela Resolução da Assembleia da República nº 88/2009, posteriormente ratificada pelo Decreto Presidencial nº 91/2009 que acolheu a publicação da Lei 109/2009 que vem transpor a "Decisão Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre o Cibercrime do Conselho da Europa".

As disposições normativas previstas nesta lei aplicam-se a todos os crimes informáticos; aos crimes cometidos por meio de um sistema informático e em relação a crimes em que seja necessário proceder à recolha das provas em suporte informático (art.º 11º nº 1). Regula também a preservação expedita de dados (art.º 12º), a revelação expedita de dados de tráfego (art.º 13º), a injunção para apresentação ou concessão do acesso a dados (art.º 14º), a pesquisa de dados informáticos (art.º 15º), a apreensão de dados informáticos (art.º 16º), a apreensão de correio eletrónico e registo de comunicações de natureza semelhante (art.º 17º), a interceção de comunicações (art.º 18º), as ações encobertas (art.º 19º) e ainda a regulação da cooperação internacional (art.º 20º ao art.º 26º).

Para além de regular a criminalidade informática e os crimes cometidos através de sistema informático, a Lei nº 109/2009 veio também esclarecer uma série de conceitos, nomeadamente o de *"dados informáticos - qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função"* (art.º 2º al. b)); *"dados de tráfego- os dados informáticos relacionados com*

[24]João Conde Correia, (…) *ob.cit.* pág. 40 e ss.

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 de serviço subjacente" (art.º 2º al. c)). Faz ainda menção ao conceito de "fornecedores de serviço" definindo-o como *"qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviços ou dos respetivos utilizadores"* (art.º 2º al. d)).

Ora, de acordo com o artigo 12º nº 1 "*a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa"*, desta forma e de acordo com a definição de "fornecedor de serviços" da presente lei, podemos entender que ficam vinculados a este regime quem armazene ou faculte estes serviços, isto é, *"não só os operadores/fornecedores de comunicações eletrónicas, mas todos os cidadãos (...) ficam vinculados ao dever de preservação expedita de dados, ficando obrigados a «assegurar a confidencialidade da aplicação da medida processual» (nº 1 e 4 do art.º 12º)*"[25].

O mesmo se aplica para o caso de injunção para apresentação ou concessão do acesso a dados previsto no art.º 14º do mesmo diploma, uma vez que poderá ser solicitado ao fornecedor de serviços o acesso ou a comunicação de outra informação para além de dados de tráfego ou de conteúdo que permita identificar por exemplo, a identidade, a morada postal ou geográfica, o número de telefone do assinante, o tipo de serviço de comunicação utilizado ou ainda qualquer outra informação sobre a localização do equipamento, sob pena de punição de desobediência.

No entanto nos nºs 5 e 6 do presente artigo é feita a ressalva de que esta medida não pode ser dirigida nem ao suspeito ou arguido do processo, de forma a acautelar o *princípio da não auto-incriminação,* nem aos sistemas de informáticos utilizados para o exercício da advocacia, das atividades médica e bancária bem como a de jornalista.

Quanto à pesquisa de dados informáticos, o legislador prevê no art.º 15º que caso se torne necessário obter de um sistema informático *"dados informáticos específicos e determinados"* com o fim de descoberta da verdade, a autoridade judiciária competente deverá ordenar por despacho que se proceda a uma pesquisa nesse sistema informático (art.º 15º nº. 1), porém os órgãos de polícia criminal poderão proceder à pesquisa sem prévia autorização da autoridade judicial caso estejamos perante crimes de terrorismo, criminalidade altamente organizada ou violenta, quando hajam indícios da prática iminente de crime que ponha em causa a integridade física ou a vida de qualquer pessoa (art.º 15º nº 3 al. b)) e ainda quando a autorização seja consentida voluntariamente pelo fornecedor do serviço.

Já, no nº 6 o legislador remete a pesquisa para as regras previstas para o regime geral das buscas previsto no art.º 174º e seguintes do CPP.

O mesmo ocorre relativamente à apreensão de dados informáticos previsto no art.º 16º nº 3 que prevê que caso sejam apreendidos dados ou documentos informáticos que possam revelar dados pessoais ou íntimos ou coloquem em causa privacidade do titular,

[25] Cfr. RITA CASTANHEIRA NEVES, *"As ingerências nas Comunicações eletrónicas em Processo Penal*", (…) *ob.cit.* págs. 234 e ss.

estes dados deverão ser apresentados a um juiz que irá ponderar, mediante os interesses no caso concreto, a sua junção ou não aos autos.

Por último, quanto aos arts.º 17º e 18º do diploma em apreço, estes vêm clarificar, primeiramente o regime relativo à apreensão do correio eletrónico e registo de comunicações de matéria semelhante, segundo o qual aplica-se "correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal", já o art.º 18º prevê o regime da interceção das comunicações. Quanto a estes preceitos iremos fazer, oportunamente a sua análise.

Em suma, este diploma pretendeu responder a uma carência legislativa no nosso ordenamento jurídico relativamente aos crimes informáticos ou crimes cometidos através de um sistema informático.

Contudo, concordamos com DÁ MESQUITA quando conclui que existe uma *"apresentação da lei esquizofrénica"*[26], pois na respetiva exposição de motivos o legislador esclarece que se pretende regular a "desadequação" da atual realidade jurídica no âmbito da prova digital, e por outro lado vem remeter a sua aplicação, ao Código de Processo Penal.

4.3. Conjugação das leis que temos:

Com a transposição dos compromissos internacionais assumidos pelo Estado português que resultaram nas leis explanadas anteriormente, e após a revisão ao Código de Processo Penal, o resultado caracteriza-se por uma total descoordenação legislativa.

Temos três diplomas distintos para a regularização da prova digital, o que propícia o aparecimento de muitas zonas cinzentas quanto à interpretação e consequente aplicação destes três diplomas.

Algumas questões que desde logo suscitam incertezas dizem respeito ao âmbito de aplicação e articulação da Lei nº 32/2008 e a Lei nº109/2009 com a regime previsto no Código de Processo Penal.

Atualmente temos dois regimes que prevêem a obtenção de dados, a Lei nº 32/2008, de 17 de Julho e o art.º 189 nº 2 do Código de Processo Penal.

Ambas as leis revogam tacitamente o que se encontra previsto no art.º 189º do Código de Processo Penal, que de acordo com JOÃO CONDE CORREIA *"as leis extravagantes sobrepõem-se àquele regime gera, que só subsiste naquilo que não foi depois especialmente regulado"*[27].

[26]PAULO DÁ MESQUITA, *"Processo Penal, Prova e Sistema Judiciário*", Coimbra Editora, 2010 *ob.cit.* pág. 98.
[27] JOAO CONDE CORREIA, *"Prova digital: as leis que temos e a lei que devíamos ter",* (…).

4.3.1. LEI Nº32/2008 E A LEI Nº 109/2009:

A relação entre a Lei nº 32/2008 e a Lei nº 109/2009 são também bastante complexas de momento, podemos distinguir duas teses relativamente à aplicação e articulação destes dois diplomas.

Primeiramente a tese minoritária que defende que a lei do cibercrime, mais concretamente "*conjugação dos arts. 11º, 12º, 13º, 14º, 16º e 18 (...) determina a revogação"* do regime de acesso aos dados que não são de conteúdo e substitui a Lei nº 32/2008, "*sobretudo, no estabelecimento dos deveres dos fornecedores de serviços de conservação e proteção desses dados, bem como das condições técnicas operativas e destruição desses dados"*[28].Essencialmente, segundo esta posição a lei 32/2008 mantem-se naquilo que não foi expressamente regulado pela lei do Cibercrime, caso contrário, manter ambos os regimes diversificados implicaria uma oneração dos crimes mais graves.

Por outro lado, a tese maioritária vem defender uma relação de complementaridade, argumentando que o próprio legislador o prevê no art.º 11º nº2 da Lei 109/2009, devendo o intérprete analisar o seu âmbito de aplicação.

Posto isto, importa agora fazer uma análise a relação entre a Lei nº 32/2008,a Lei nº 109/2009 e o Código de Processo Penal.

4.3.2. A LEI Nº 32/2008 E O CÓDIGO DE PROCESSO PENAL (a localização celular):

Quanto a estes diplomas existem algumas dissonâncias, porém importa primeiramente definir os diferentes tipos de dados que poderão ser alvo de apreensão: os dados de base, os dados de tráfego e os dados de conteúdo.

Os dados de base dizem respeito à identificação dos emissores ou destinatários a uma rede pública de comunicações, assim estes não são suscetíveis de revelarem uma comunicação. São dados prévios e instrumentais para o acesso ao serviço, por exemplo dados como o nome, a morada, e os dados que aquela empresa fornece para uma interligação à rede e ou ao serviço de comunicações como o nome de utilizador e a password.

Já os dados de tráfego são dados essenciais para que haja o estabelecimento de uma ligação, por exemplo a localização do utilizador, localização do destinatário, duração da utilização, data e hora.

Por seu turno, os dados de conteúdo, são os que dizem respeito ao conteúdo da mensagem eletrónica.

Desta feita, se fizermos uma análise à Lei nº 32/2008 e ao Código de Processo Penal, a principal incongruência diz respeito aos dados de tráfego, mais propriamente os dados de localização celular. Isto porque o art.º 189º nº2 do CPP prevê que *"a obtenção e junção aos autos de dados sobre a localização celular*[29] *ou de registos da realização*

[28] PAULO DÁ MESQUITA, "Processo Penal, Prova e Sistema Judiciário", Coimbra Editora, 2010 *ob.cit.* pág. 123

[29] MANUEL DA COSTA ANDRADE, entende que "*o preceito se reporta apenas aos chamados autênticos dados de comunicação ou de tráfego. Vale por dizer que, à vista do regime ora vigente, só será legitimo obter e recolher dados de localização e de tráfego relativos a uma comunicação efetiva ou, ao menos,*

de conversações ou comunicações só podem ser ordenadas ou autorizadas em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no nº3 do art.º 187º e em relação a pessoas referidas no nº 4 do mesmo artigo", por outro lado a Lei nº 32/2008 prevê que a obtenção de dados pode ser ordenada por despacho do juiz de instrução quando esta seja indispensável para a descoberta da verdade ou que a prova seria impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves.

Para além disto, com a reforma de 2007 foi introduzido o art.º 252º-A "localização celular", segundo este artigo *" As autoridades judiciárias e as autoridades de policia criminal podem obter dado sobre a localização celular quando eles forem necessários para afastar o perigo de vida ou de ofensa à integridade física grave*", assim, feita a conjugação dos dois artigos previstos no Código de Processo Penal podemos concluir que para que seja possível a obtenção de dados de localização celular, não é necessário uma autorização judicial desde que estejamos perante uma situação que seja necessário afastar o perigo de vida ou de ofensa à integridade física.

No entanto, de acordo com a teoria maioritária a Lei 32/2008, encontra-se parcialmente revogada pela Lei 109/2009.

Nesta senda, o Acórdão do Tribunal da Relação de Évora, de 20 de Janeiro de 2015[30], debruça-se sobre esta questão da localização celular, segundo o qual *"Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis – processualmente úteis – de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189º, n. 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real. (...) Agora coexistem três realidades distintas através do acrescento da obtenção de dados de localização celular "conservados" por via da Lei nº 32/2008. (...). Os requisitos do número 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa." Uma vez que "O regime processual da Lei nº 32/2008 constitui relativamente aos dados "conservados" que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009".*

Posto isto, relativamente à temática da localização celular, devemos fazer uma articulação conjunta dos três diplomas, assim sendo nos termos do art.º 14º da Lei 109/2009 não existe uma necessidade de intervenção judicial prévia para a informação que se encontre armazenada.

Em suma, não se justifica a existência de três diplomas distintos para a regulação de dados que são transversais a todo o tipo de comunicações. Neste caso, o legislador dispersou ao invés de proceder a uma uniformização normativa.

---

tentada entre pessoas. (...) não cabem aqui os dados de localização ou de tráfego correspondente à «comunicação entre máquinas», dados cuja obtenção é tornada possível pelo simples facto de se manter o aparelho em stand-by. Tal valerá por exemplo para as operações de IMSI e IMEI à margem duma efetiva comunicação telefónica. E por maioria de razão para os casos de SMS silencioso, in MANUEL DAS COSTA ANDRADE, "Bruscamente no Verão passado; a Reforma do Código de Processo Penal, observações criticas de uma lei que podia e devia ter sido diferente", Coimbra Editora 2009 *ob.cit.* pág. 187.

[30] Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument

4.3.3. LEI 109/2009 E O CÓDIGO DE PROCESSO PENAL:

A Lei do Cibercrime regula muito mais que a cibercriminalidade, esta aplica-se em casos que sejam necessários proceder à recolha de provas que se encontrem em suporte informático ou em casos em que ocorra investigação de crimes praticados através de um sistema informático.

Não há dúvida que a Lei 109/2009 constitui uma verdadeira inovação legislativa no ordenamento jurídico português, porque veio regular uma realidade que não tinha até então tinha sido negligenciada pelo nosso legislador, a criminalidade cometida através de sistemas informáticos ou em casos que seja necessário proceder à recolha de provas em suporte digital.

Após esta clarificação de aplicação entre estas duas legislações avulsas, cabe-nos agora destacar as principais incoerências entre a Lei do Cibercrime e o regime previsto no Código de Processo Penal.

Primeiramente, uma das principais críticas relativas à equiparação do correio eletrónico em curso ao regime das escutas telefónicas diz respeito ao estrito catálogo de crimes previstos (crimes com pena de prisão superior a três anos, art.º 187º nº1 CPP) o que restringia consideravelmente o acesso a estes ficheiros no decurso da investigação de crimes informáticos e até mesmo na obtenção da prova digital.

Contudo, fruto da previsão do art.º 17º da Lei 109/2009 passa a prever um âmbito mais vasto de aplicação, permitindo a obtenção do correio eletrónico sempre que esteja em causa um crime cometido através de um sistema informático ou em relação ao qual seja necessário proceder uma recolha de prova que se encontre em suporte digital (art.º 11º nº1).

De acordo com esta disposição legal "*quando no decurso de uma pesquisa informática ou outro acesso legitimo a um sistema informático, forem encontrados,* ***armazenados,*** *nesse sistema informático ou noutro a que seja permitido o acesso legitimo 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 da correspondência previsto no Código de Processo Penal".*

Desta forma, no regime previsto no art.º 179º do CPP o legislador exige, sob pena de nulidade, que o juiz poderá autorizar por despacho a apreensão de correspondência[31] quando esteja em causa, (1) a correspondência dirigida ou expedida pelo suspeito ou arguido, mesmo que esteja sob nome ou pessoa diversa; (2) um crime punível com pena de prisão superior, no seu máximo, a três anos; (3) uma diligência que se revele indispensável para a descoberta da verdade ou para a prova (nº 1 art.º 179º).

Estabelece ainda a proibição da apreensão e qualquer outra forma de controlo da correspondência entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que a correspondência em causa constitui objeto ou elemento de um crime (art.º 179º nº 2) e finalmente, determina que o juiz que tiver autorizado ou ordenado a diligência, deverá ser o primeiro a ter o conhecimento do conteúdo da correspondência

apreendida, procedendo ao seu aditamento ao processo, caso esta se revele pertinente ou, pelo contrário, ordenar a sua restituição[32] a quem de direito, impedido, consequentemente a sua utilização como meio de prova e a respetiva divulgação, uma vez que ficará vinculado a um dever de segredo ao que tiver tomado conhecimento.

Explanados ambos os diplomas, é necessário uma articulação entre o que se encontra previsto no CPP (art.º 179º) e a Lei nº 109/2009 (art.º 17º), assim na senda de RITA CASTANHEIRA NEVES[33], a remissão para o regime de apreensão de correspondência (art.º 179º CPP) não abrange a alínea c) do nº 1, não sendo necessário para a aplicação da Lei do Cibercrime a verificação, no caso concreto, de um crime punível com pena de prisão superior a três anos, ou seja, é aplicado o art.º 17º aplica-se ao catálogo de crimes previsto no respetivo diploma (art.º 11º nº 1 da Lei 109/2009).

Por último, relativamente a este diploma há que fazer uma análise ao art.º 18 que regula a interceção das comunicações relativas a crimes previstos neste diploma, ou ainda crimes cometidos através de um meio informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando estes se encontrem previstos no art.º 187º do CPP.

Tratando-se de uma ingerência nas comunicações o legislador restringiu a sua aplicação a um elenco de crimes mais estrito, de forma a salvaguardar a privacidade dos visados.

Relativamente aos artigos anteriores tratava-se de uma ingerência nos ficheiros ou dados digitais que resultam da comunicação, mas que se encontram armazenados, isto é, dizem respeito a um segundo momento da comunicação, quanto ao que se encontra previsto no art.º 18º a intervenção diz respeito à comunicação em si mesma.

De acordo com RITA CASTANHEIRA NEVES *"a ratio para o estabelecimento deste regime foi precisamente a de prevenir a discrepância que resultaria de às próprias mensagens de correio eletrónico que resultaram de uma comunicação serem aplicados os requisitos exigíveis para uma situação de intromissão na esfera da privacidade ao nível da autodeterminação informacional e aos respetivos dados de tráfego e de localização serem aplicados sempre, em qualquer situação, as restrições tidas em conta pela proteção da privacidade e pela proteção do segredo das comunicações".*

Já o nº 2 do art.º 18º prevê que quer a interceção, quer o registo de transmissões de dador informáticos só podem ser autorizados, por despacho fundamento do juiz de instrução e mediante requerimento do Ministério Público, durante o período de inquérito quando a medida se revele indispensável para a descoberta da verdade ou caso a prova seria impossível ou muito difícil de obter de outra forma.

Portanto, para que haja uma interceção das comunicações, contrariamente ao regime previsto quer para a preservação expedita de dados (art.º 12º), para revelação expedita de dados de tráfego (art.º 13º), quer para a injunção para a apresentação ou concessão do acesso a dados (art.º 14º), os órgãos de policia criminal não podem intervir

[32] De acordo com RITA CASTANHEIRA NEVES, só em alguns casos é que ocorre uma verdadeira restituição da correspondência apreendida, uma vez que "…as informações objeto da diligência não deixam geralmente de estar com a pessoa visada, tendo-se apenas procedido a uma cópia", cfr RITA CASTANHEIRA NEVES, "*As ingerências nas Comunicações eletrónicas em Processo Penal*", (…).

[33] RITA CASTANHEIRA NEVES, "As ingerências nas Comunicações eletrónicas em Processo Penal"(…).

diretamente pois é necessário um despacho fundamentado pelo juiz de instrução e mediante inquérito do Ministério Público.

Tratando-se de uma medida mais lesiva para a privacidade e estando em causa a comunicação em si mesma, ou seja, há uma interceção em tempo real da comunicação, o legislador foi mais rigoroso quanto aos seus requisitos.

No nº 3 do art.º 18 prevê que a interceção da comunicação poderá destinar-se aos dados de conteúdo das comunicações ou apenas a recolha e registo dos dados de tráfego[34], contudo o despacho fundamentado do juiz deve especificar o âmbito de acordo com as necessidades da investigação.

Existe uma proteção acrescida uma vez que estamos perante uma interceção da comunicação em tempo real, desta forma os dados gerados pela comunicação encontram-se protegidos pelo direito à inviolabilidade das comunicações previsto constitucionalmente pelo direito à privacidade.

Por último, o nº 4 desta norma faz uma remissão para o "regime da interceção e gravação de conversações ou comunicações telefónicas" previsto no Código de Processo Penal nos artigos 187º a 190º[35].

Tendo em conta esta remissão é necessário clarificar o seu âmbito, primeiramente, no que diz respeito ao art.º 187º a remissão feita na Lei do Cibercrime não se aplica ao catálogo de crimes previstos no art.º 187º nº1, uma vez que o art.º 18º nº 1 al. a) regula o âmbito de aplicação do diploma. Quanto ao nº2 poderá haver aplicação do art.º 187º para a determinação da competência para a autorização da ingerência em casos de crimes de: terrorismos, criminalidade violenta ou altamente organizada, sequestro, rapto ou tomada de reféns, crimes contra a identidade cultural e integridade pessoal, crimes contra a segurança do Estado, falsificação de moedas ou títulos equiparados a moeda e ainda relativamente a crimes abrangidos por convenção sobre segurança e navegação aérea ou marítima.

No que respeita às interceções das comunicações previstas no art.º 18º além de estar sujeito aos requisitos previstos no diploma da cibercriminalidade é necessário que estejam preenchidos os seguintes pressupostos previstos no Código de Processo Penal: no nº 4 do art.º 187º encontra-se previsto que a interceção só pode ser autorizada contra o suspeito ou o arguido, pessoa que sirva de intermediário, desde que haja fundadas razões de que esta recebe ou transmite mensagens destinadas ou provenientes do suspeito ou do arguido, e contra a vitima de crime, mediante o respetivo consentimento (efetivo ou presumido).

O nº 5 do art.º 187º proíbe a interceção e gravação de conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objeto ou elemento do crime. A interceção poderá ter a duração

---

[34] "*dados 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*." Art.º 2º al. c) Lei nº 109/2009.

[35] Não é feita uma remissão para o regime previsto no art.º 189º, uma vez que a sua aplicação foi praticamente foi substituída pelo art.º 18º, assim em casos que estejam previstos como crime nº nº1 deste artigo e em casos em que o crime seja cometido por meio de um sistema informático ou em relação qual seja necessário proceder à recolha de prova em suporte eletrónico, deverá aplicar-se o art.º 18º da Lei 109/2009, nos restante elenco de crimes previsto no art.º 187º, deverá aplicar-se o regime previsto no art.º 189º do CPP.

máxima de 3 meses, podendo ser renováveis por períodos sujeitos ao mesmo limite desde que se verifiquem os respetivos requisitos de admissibilidade (art.º 187º nº 6.), só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de interceção de meio de comunicação utilizado por pessoa referida no nº 4 e que seja indispensável para a prova do crime (art.º 187º nº 7) e por último, os suportes técnicos das conversações e respetivos despachos que as fundamentam devem ser juntas, mediante despacho judicial, ao processo em que devam ser utilizadas como prova (nº 8 art.º 187º).

Relativamente às formalidades do processo de interceção das comunicações o artigo 18º da Lei nº09/2009, segue o que se encontra previsto no art.º 188º do CPP, sob pena de nulidade previsto no art.º 190º do CPP.

Posto isto, é do nosso entender que a Lei do Cibercrime além de inovadora, vem regular uma realidade que até então estava carecida, a recolha de prova em suporte eletrónico.

Vem desde logo, estabelecer um conjunto de conceitos que até então estavam carentes de definição, nomeadamente o de "dados de tráfego", prevê um novo regime, para o acesso e preservação de dados, distingue, a nível do correio eletrónico, a comunicação em si mesma, dos dados resultantes da comunicação e que se encontram armazenados, fazendo no fundo uma divisão da comunicação em dois momentos tendo cada um deles pressupostos e proteções distintas.

Destarte, com a entrada em vigor quer da Lei 32/2008, quer da Lei nº 109/2009, o que foi discutido supra relativamente à interceção do correio eletrónico e ao respetivo regime previsto no art.º 189º nº 1 e 2, passou a assumir um carácter subsidiário, assim, quando estejamos perante um crime previsto e punido pelo art.º 187º CPP, mas que seja necessário proceder à recolha de prova que se encontre em suporte informático deverá aplicar-se a Lei nº 109/2009, em todos os restantes casos aplica-se o previsto no art.º 189º CPP.

Desta forma, partilhamos da mesma opinião de JOAO CONDE CORREIA, quando este afirma que "*não se compreende, por isso, porque é que o legislador não o revogou formalmente, expurgando-o daquilo que não tem aplicação e impedindo que se continue a invocar a sua vigência. A sua manutenção formal só pode ser perniciosa*".[36]

[36] JOÃO CONDE CORREIA, "*Prova digital: as leis que temos e a lei que devíamos ter"*, Revista do Ministério Público 139: Julho: Setembro 2014

5. O caso particular dos SMS

5.1. Considerações gerais

As SMS são uma realidade permanente no nosso quotidiano, grande parte da população utiliza reiteradamente este meio de comunicação, desta forma urge uma resposta eficiente por parte do processo penal a este meio de prova.

Na atual legislação nacional não há uma menção perentória relativamente aos SMS, o que tem suscitados algumas questões no ceio da jurisprudência. Vamos, por isso tecer algumas considerações sobre este particular meio de comunicação.

Primeiramente, é inquestionável que os SMS (*Short Message Service)* constituem um meio de comunicação e por isso subsumível ao regime previsto para este meio de prova (art.º 189º do CPP e Lei nº 109/2009).

Desta feita, o tratamento que devemos dar aos SMS é o mesmo que o do correio eletrónico dividindo-se igualmente em dois momentos distintos: o primeiro momento pauta-se pela transição da mensagem entre o emissor e o recetor e a respetiva chegada ao domínio do destinatário (art.º 18º da Lei 109/2009), neste momento estamos perante uma comunicação cuja interceção só pode ser realizada durante inquérito, mediante autorização judicial a requerimento do Ministério Público e ainda que a diligência seja indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter. Todavia, ainda existem na doutrina e na jurisprudência vozes dissonantes quanto ao respetivo processo deste meio de obtenção de prova.

Posteriormente, num segundo momento, após a leitura da mensagem, a SMS deverá ser submetida ao regime geral da correspondência (art.º 179º CPP *ex vi* art.º 179º CPP).

Quanto à aplicação pela jurisprudência esta tem sido contraditória ao que se encontra previsto no processo penal, dentro destas aplicações é de destacar o Acórdão do Tribunal da Relação de Guimarães, de 15 de Outubro de 2012[37], segundo esta peça "(…) *Enquanto a mensagem não for "aberta" e lida pelo destinatário, a transmissão da comunicação não está completa. Durante todo esse tempo a sua interceção está sujeita às regras das interceções das comunicações telefónicas. O bem tutelado é o direito à reserva da vida privada, que só pode ser postergado mediante prévia decisão judicial. Nada de substancial, quanto aos valores tutelados, diferencia uma sms da demais correspondência trocada entre particulares, sejam cartas, telegramas, encomendas, ou qualquer outra forma de correio.*

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

[37] Disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/d7e67584752588c980257aa0004607bc?OpenDocument

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.".

Embora estejamos de acordo que uma vez findo o processo comunicacional, através da leitura da mensagem, a comunicação bem como a respetiva tutela cessam e o regime a seguir seria o regime geral das buscas previsto no art.º 174º e seguintes do CPP. não foi esta a posição assumida pelo nosso legislador, pois a SMS após leitura constitui uma mensagem sujeita ao regime geral da correspondência.

Por outro lado, o Acórdão do Tribunal da Relação do Porto, de 27 de Janeiro de 2010, teceu as seguintes considerações[38]: *""I - A leitura feita pela PJ de mensagem registada no cartão SIM de um telemóvel que já entrou na esfera de domínio do destinatário, não se configura como interceção de conversação ou comunicação telefónica para efeitos da aplicação dos artigos 187º e 188º, nem lhe é aplicável a extensão enunciada no artigo 189º nº1, todos do CPP. II - A mensagem via telemóvel já recebida deverá ter o mesmo tratamento da correspondência escrita, que circula através do tradicional sistema postal: recebida, mas ainda não aberta pelo destinatário, aplicar-se-á, à respetiva apreensão, o estabelecido no artigo 179º do CPP; recebida, aberta e guardada pelo destinatário, já não beneficiará do regime de proteção da reserva da correspondência e das comunicações, podendo ser apreendida para valer como mero documento escrito"*.

O presente acórdão assumiu uma posição tripartida da comunicação eletrónica, que se revela desadequada e desproporcional, não só porque o legislador quer no regime geral (art.º 189º CPP) quer no regime especial (art.º 17º e 18º da Lei do Cibercrime) assume, claramente, uma visão bipartida, ou seja, a vida da mensagem eletrónica é dividida em dois momentos o de trânsito e o momento de armazenamento, mas também porque, como abordado anteriormente, uma divisão tripartida suscita elevadas dificuldades práticas a nível da apreensão.

Muito embora não concordemos com a solução legal prevista pelo legislador, porque no nosso entendimento privilegia irrefletidamente os documentos eletrónicos em detrimento do correio tradicional, isto não quer dizer que os tribunais possam fazer uma aplicação corretiva da legislação, para que haja uma produção de prova válida o SMS segue os trâmites previstos no art.º 18º da Lei do Cibercrime quanto à sua interceção e caso se encontre armazenado o regime da correspondência art.º 179º CPP *ex vi* do art.º 17º da Lei do Cibercrime.

[38] Disponível em: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/68fdcdf35dc62b6e802576c40041c799

6. A LEI QUE DEVERÍAMOS TER

6.1. As incongruências legislativas, falhas e omissões.

A Revisão de 2007, não foi aproveitada pelo nosso legislador para regulação e dos meios de prova emergentes, MANUEL DA COSTA ANDRADE afirma que esta Revisão ao Código de Processo Penal foi uma *"oportunidade perdida de, pela primeira vez, assegurar reconhecimento e tratamento adequado aos problemas polarizados pelo uso e abuso das telecomunicações, em geral. E, por vias disso, continuámos atavicamente amarrados a uma equacionação dos problemas a partir das escutas telefónicas e do seu regime, no essencial, pensado e estruturado na perspetiva do velho telefone fixo"*.[39]

A matéria da prova digital encontra-se regulada em três diplomas distintos: o Código de Processo Penal, a Lei nº 32/2008, de 17 de Julho, e a Lei 109/2009, de 15 de setembro, o legislador ao invés de optar pela centralidade e clareza legislativa, optou por uma legislação difusa e dúbia.

No Código de Processo Penal, como visto anteriormente, estendeu-se o regime das escutas telefónicas para outros meios técnicos distintos do telefone, tais como o correio eletrónico, as SMS e meios equivalentes, mesmo que estes se encontrem lidos e armazenados no dispositivo (art.º 189º nº 1 CPP).

Neste artigo o legislador seguiu a via de que mesmo já lido a mensagem merece tutela da inviolabilidade das comunicações, no entanto isto veio onerar significativamente a investigação criminal em relação ao regime previsto para a correspondência.

Por outro lado, previu ainda na Lei 109/2009 a qual *"veio acrescentar mais um apertado e desnecessário nó górdio."* [40], as disposições normativas deste diploma vêm revogar parcialmente o regime previsto no Código de Processo Penal relativamente aos crimes que sejam praticados por meio de um sistema informático e, ainda aos crimes em que seja necessário proceder à recolha do de prova que se encontre em formato digital.

Deste diploma, iremos salientar o art.º 17º, no qual o legislador deixou bem clara a posição de que a mensagem de correio eletrónico ou outro registo de comunicação semelhante após lida merece a tutela da inviolabilidade, submetendo ao regime da correspondência previsto no regime geral (art.º 179º CPP) sendo assim necessário o respetivo despacho judicial.

Já a Lei 32/2008, veio regular a conservação e a transmissão dos dados de tráfego e de localização, assim como os dados necessários para a identificação do assinante do serviço.

No seu art.º 9 estabelece um catálogo restrito de crimes relativamente aos quais pode haver a transmissão dos dados, mas sempre mediante despacho judicial e caso

---

[39] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão passado; a Reforma do Código de Processo Penal, observações criticas de uma lei que podia e devia ter sido diferente"*, Coimbra Editora 2009 *ob.cit.* pág. 97 e ss.

[40] JOÃO CONDE CORREIA, "*Prova digital: as leis que temos e a lei que devíamos ter",* Revista do Ministério Público 139: Julho: Setembro 2014

estejamos perante um meio indispensável para a descoberta da verdade ou que sem o qual seria impossível ou muito difícil de obter a prova.

Posto isto, o legislador veio duplicar o que já se encontrava previsto no regime geral fugindo à centralidade normativa ideal para uma aplicação eficaz.

Em suma, a técnica legislativa para a regulação deste meio de prova não foi a mais adequada, inclusivamente, a Lei nº 32/2008 e a Lei nº 109/2009, ficaram muito aquém, originando uma disseminação e confusão desta matéria.

Desde já, o legislador conferiu uma acrescida proteção às mensagens de correio eletrónico ou outra forma de comunicação equiparável, contrariamente ao regime previsto para a correspondência tradicional.

Por outro lado, não fez uma previsão expressa para os crimes de injúria, ameaça, coação e devassa da vida privada quando cometidos por meio eletrónico, de acordo com o art.º 187º há uma previsão para estes tipos legais, mas quando cometidos através do telefone.

Perante esta realidade, e feita a análise da legislação que temos importa agora discutir qual a legislação que deveríamos ter.

6.1.1. O correio eletrónico recebido e lido.

Tendo em conta a análise tecida anteriormente, fica claro que a técnica legislativa do nosso legislador se revelou desadequada para responder os desafios provocados pela era digital que vivemos e também na concretização dos compromissos internacionais assumidos face às instituições europeias.

O legislador poderia e deveria ter acautelado as exigências penais e de investigação criminal de uma forma mais clara e unívoca, no entanto, não é isso que temos fruto das revisões ao Código de Processo Penal, a transposição da Diretiva nº 2006/24/CE do Parlamento Europeu e do Conselho de 15 de Março e a Decisão Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro que culminaram com o surgimento de dois diplomas distintos (Lei nº 32/2008 e o da Lei nº 109/2009, explanados anteriormente).

Uma das questões mais discutidas no seio da doutrina, relativamente ao novo regime da prova digital, diz respeito à tutela conferida pelo processo penal ao correio eletrónico que se encontra armazenado e lido.

Como mencionado anteriormente, e partilhando o entendimento de RITA CASTANHEIRA NEVES, entendemos que o correio eletrónico só cumpre a sua função de comunicação após a ser lido, isto quer dizer que quando o a mensagem eletrónica chega à esfera de domínio do destinatário, mas jaz lá à espera de ser lida, neste compasso de espera entre a chegada à caixa e correio e a respetiva leitura estamos perante uma comunicação eletrónica sujeita ao regime do art.º 189º do CPP.

Após a sua abertura e leitura da mensagem eletrónica qual o regime que deveríamos ter em conta? É uma polémica desnecessário que podia e deveria ter sido prevista pelo legislador de forma inequívoca.

De acordo com MANUEL DA COSTA ANDRADE *"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 com um normal escrito"*.

Partilhamos da mesma linha de pensamento deste autor, no entanto, dada a parca clareza legislativa, e visto que não há uma delimitação expressa da extensão da comunicação eletrónica, porém no art.º 17º da Lei nº 109/2009 o legislador recorre à expressão "armazenados" que implica que o destinatário da mensagem eletrónica já tomou conhecimento da mesma.

O legislador conferiu, portanto, ao correio eletrónico recebido, lido e armazenado um "*plus de proteção a arquivos que já foram comunicações, em nome da salvaguarda a privacidade da autodeterminação informacional, remetendo para o regime da correspondência"*[41].

Se fizermos esta interpretação literal, é evidente a desigualdade de grau de proteção entre os documentos que constituam meio de prova e se encontrem em formato digital, dos meios de prova que se encontrem em formato de papel.

No entanto, e na senda de JOÃO CONDE CORREIA se fizermos "*uma leitura coerente, que acentue as inevitáveis semelhanças com os escritos tradicionais e as suas necessidades de tutela, tenderá todavia, apesar daquele elemento gramatical, a excluir este correio, considerando-o, como um mero documento e facilitando a sua apreensão: será para o efeito suficiente a intervenção legitimadora do magistrado do Ministério Público (art.º 16º da Lei nº 109/2009)"*[42].

Para efeitos práticos *"o Ministério Público pode apreender uma carta guardada num cofre, mas não um email guardado num computador"*.

De facto, não há necessidade de uma tutela acrescida e não se justifica este favorecimento em relação aos restantes escritos. Todavia não é isto que se encontra previsto na lei, não podemos fazer uma interpretação que viola claramente o sentido seguido pelo legislador.

A posição assumida pelo legislador neste preceito normativo, é de que findado o processo de comunicação continua a haver uma necessidade de tutela da inviolabilidade da correspondência (art.º 34º CRP).

Em suma, a solução legislativa para o correio eletrónico armazenado é a de que continuamos no âmbito da tutela da correspondência como tal subsumida ao regime geral, no nosso entendimento a mensagem eletrónica já recebida e lida deveria ser encarada como um mero escrito, pois é disso que se trata, visto que o seu fim comunicacional foi atingido. No fundo a interceção do correio eletrónico como meio de prova, poderia ser dividida em dois momentos, o primeiro pautava-se pela ingerência enquanto este se encontrar e trânsito e posteriormente, quando este deixar de constituir uma comunicação recebido e lido, poderia ser alvo de busca nos termos gerais.

---

[41] RITA CASTANHEIRA NEVES, "*As ingerências nas Comunicações eletrónicas em Processo Penal",* Coimbra editora, 2011, *ob.cit.* pág. 276 e ss.

[42] JOÃO CONDE CORREIA, *"Prova digital: as leis que temos e a lei que devíamos ter"*, Revista do Ministério Público 139: Julho: Setembro 2014 *ob.cit.* pág. 40 e ss.

6.1.2. O que fazer quanto aos crimes de injúrias, ameaças, coação e devassa da vida privada quando cometidos por meio eletrónico?

Esta é uma das grandes falhas do legislador nacional, ao invés de fazer uma regularização geral dos meios de obtenção de prova, optou por uma regulação mais restritiva a certos casos.

O catálogo de crimes previsto no regime das escutas telefónicas do Código de Processo Penal não acautela os casos de injúrias, ameaças, coação e devassa da vida privada cometidos através de um meio informático.

Já a Lei nº 109/2009 no seu art.º 18º nº 1 prevê que a interceção da comunicação ocorre em processos relativos a crimes: (1) estejam previstos no respetivo diploma; (2) sejam cometidos através de um sistema informático, ou em relação aos quais seja necessário proceder à recolha em suporte digital, quando se encontrem previstos no art.º 187º do CPP.

Quanto a esta falha, BENJAMIM SILVA RODRIGUES[43], propõe um único catálogo de crimes que seria aplicável a toda a monitorização dos fluxos informacionais e comunicacionais, por outro lado, para os crimes de injúrias, ameaças, coação e devassa da vida privada, seriam previstos inclusive *"quando cometidos através de redes postais ou redes e serviços de comunicações eletrónicas publicamente acessíveis"*.

Por outro lado, JOÃO CONDE CORREIA, entende que uma leitura literal do tipo legal do art.º 18º nº 1 seria inadmissível, este autor afirma que os casos previstos no art.º 18º nº 1 a) não dependem de um outro requisito adicional "*por isso autonomizou as duas alíneas do referido artigo"*, por outro lado, a remissão operada na al. b) desta norma *"deverá, numa interpretação atualista, incluir os crimes de injúria, ameaça, coação ou devassa da vida privada cometidos através de sistema informático"*.[44]

Portanto, não nos parece ser a mais acertada a posição de BENJAMIM SILVA DIAS, uma catalogação geral para toda a monitorização de fluxos não seria o mais recomendável. Não nos podemos esquecer que estão em causa diferentes níveis de lesividade, toda a proteção deverá ter em conta um grau de proporcionalidade e necessidade, assim em casos em que esteja em causa a palavra falada, esta terá uma maior necessidade de tutela que a palavra escrita, como vimos anteriormente.

Contudo, ao nível da jurisprudência o Tribunal da Relação de Évora, de 07 de Dezembro de 2012, proferiu o seguinte: *"Tendo no decurso do inquérito sido participado contra desconhecidos um crime de difamação agravada praticada através da Internet, e visando-se apurar dados de tráfego de comunicações eletrónicas (dados relativos às ligações do computador de um agente a um fornecedor de serviço de acesso à Internet), cujo acesso só é possível, nos termos legais, através de autorização do JIC, o regime aplicável é o prevenido no art.º 187º, por remessa do art.º 189º do C.P.Penal. (...) tal conclusão decorre exatamente da equiparação do crime de difamação ao crime de injúria, sob pena de, doutra forma, a prática dum crime de injúrias por via telemática só*

[43] BENJAMIM SILVA RODRIGUES, "*Das escutas telefónicas - A monitorização dos fluxos informacionais e comunicacionais, Tomo I*", Coimbra Editora, 2008, *ob.cit,* pág. 540 e ss.
[44] JOÃO CONDE CORREIA, "*Prova digital: as leis que temos e a lei que devíamos ter*", (…) *ob.cit.* pág. 40 e ss.

ser possível aquando duma videoconferência, situação completamente restritiva e injustificada quando num qualquer crime de difamação em causa estão precisamente os mesmos bens jurídicos que no crime de injúrias. O correio eletrónico nunca seria possível de intercetar e gravar porque, por natureza, lhe falta a "presencialidade", elemento crucial para a verificação do mencionado crime de injúrias."

Este Acórdão faz uma equiparação entre tipos legais, a difamação agravada e a injúria, sob pena de o crime de difamação não ser previsto neste elenco para que seja admissível a sua produção de prova.

Porém, a posição de JOÃO CONDE CORREIA parece-nos mais razoável e realista face ao regime geral previsto no nosso ordenamento jurídico pois somente através de uma interpretação atualista da alínea e) do nº do art.º 187º podemos subsumir os crimes de injúria, ameaças, coação e devassa da vida privada quando cometidos por meio eletrónico.

6.1.3. O SMS lido e armazenado

Dentro desta temática há duas questões que urgem resposta:

a) Como e quem pode fazer a respetiva apreensão?
b) É possível a livre disposição do conteúdo da mensagem?

Quanto à primeira questão, entendemos que a comunicação finda após a leitura do conteúdo da mensagem eletrónica, estamos perante um mero escrito subsumível ao regime geral das buscas e da apreensão previsto no CPP (artsº. 174º e ss.).

No entanto a Lei do Cibercrime remete, à semelhança do correio eletrónico, para o regime da correspondência plasmado no art.º 179º do CPP, se não estamos mais perante uma comunicação qual o sentido desta remissão? No nosso entendimento não existe razões para tal, a SMS depois de concretizar o seu propósito comunicacional deverá ser encarado como um mero escrito[45] e como tal subsumível ao respetivo regime (art.º 15º da Lei do Cibercrime e regime geral das buscas e das apreensões art.º 174º e seguintes do CPP).

A carta após aberta e colocada no respetivo envelope é um escrito suscetível numa busca de apreensão pelos órgãos de policia criminal, não faz sentido que às comunicações realizadas através de um meio informático se atribuía um tratamento diferente.

Respondendo à segunda questão, devemos ter em conta que estamos perante uma tutela que visa a proteção da reserva da vida privada, no entanto após a entrada da mensagem no domínio do destinatário nada impede que este disponha do seu conteúdo,

[45] Quanto às publicações em blogs ou plataformas como o Facebook o Acórdão do Tribunal da Relação do Porto, de 13 de Abril de 2013, estamos perante um mero escrito *" (...) a questão não se dirime pela denominada Lei do Cibercrime (Lei 109/2009 de 15/09), na medida em que a postagem efectuada pela arguida a sua página de Facebook constitui um mero documento, apreensível por qualquer pessoa, pelo que a assistente se limitou a extrair uma cópia do mesmo, não se tratando assim de uma questão relativa a criminalidade informática, ou recolha de prova em suporte eletrónico, não sendo por isso o dito documento enquadrável para o conceito de comunicações alusivo naquela Lei.",* disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument&Highlight=0,109%2F2009

ou seja, se a vítima do crime apresentar a mensagem como prova da pática do ilícito, não se justifica a existência de um despacho judicial.

Ora, como mencionado anteriormente a entrada da mensagem no telemóvel e a leitura da mesma, a SMS, no nosso entendimento deveria constituir um mero documento escrito[46] em suporte digital, e como devemos ter em conta que o direito da reserva da vida privada é um bem disponível pelo qual o lesado poderá dispor deste mesmo direito.

Assim sendo, partilhamos da posição que o regime previsto para o SMS, à semelhança do correio eletrónico deveria ser o seguinte: a SMS após lida poderia ser alvo de busca e apreensão nos tramites gerais, ou seja, de acordo com o art.º 15º nº 3 a) da Lei do Cibercrime, por outro lado, os órgãos de policia criminal poderiam proceder à respetiva busca, sem autorização da autoridade judiciária, quando a mesma fosse voluntariamente consentida, só faz sentido a necessidade de despacho judicial quando os dados pretendidos não estão acessíveis ou quando não são espontaneamente facultados por quem pode dispor deles livremente. Caso isto ocorra é necessária a intervenção do juiz de instrução que terá que fazer uma ponderação entre valores conflituantes.

Nesta senda, o Acórdão do Tribunal da Relação de Guimarães, de 15 de Outubro de 2012, segundo o qual *"Afigura-se desproporcionada a ideia de que o legislador pretendeu impor, a cada cidadão proprietário de um computador pessoal, que só possa fornecer a um tribunal os dados que nele possui depois de prévia autorização do juiz. Seria um entendimento pouco harmonioso com teleologia da lei, que visa a proteção do proprietário do sistema informático contra atentados de terceiros à privacidade dos seus próprios dados (e não a proteção dos terceiros)."*

Em suma, a remissão da Lei do Cibercrime para o regime da apreensão da correspondência não faz sentido, já que não estamos mais perante uma comunicação. Assim, no âmbito de uma busca os órgãos de policia criminal poderiam proceder à respetiva apreensão, dispensando um despacho judicial.

Na prática como se concretiza esta apreensão? No sistema judicial alemão é reconhecida a possibilidade de busca clássica seja através da apreensão do aparelho, seja através da cópia dos ficheiros que nele se encontram, assim sendo, de acordo com MANUEL DA COSTA ANDRADE[47], entende que este mecanismo se aplica igualmente para a informação, conteúdos e dados de comunicação, que se encontram guardados no cartão do telemóvel, e dizem respeito quer às comunicações por ele realizadas, quer às mensagens escritas (SMS).

---

[46] *"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 protecção da reserva da correspondência e das comunicações.",* Acórdão do Tribunal da Relação de Évora, de 07 de Abril de 2015, disponível em : http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/ad8068a8c8f9b3c080257e2e00356d33?OpenDocument&Highlight=0,189%C2%BA,CPP

[47] MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão passado; (...) ob.cit.* pág. 156 a 160.

Considerações Finais

Ao longo da presente dissertação, na qual analisamos o regime do processo penal previsto para o correio eletrónico e meios de comunicação equiparáveis como as SMS, fomos colocando várias interrogações e tentamos responder às mesmas.

O legislador português propiciou uma indesejável desordem normativa do regime previsto para a prova digital, apesar de ser uma realidade recente só em 2009 se previu verdadeiramente o regime jurídico para este meio de prova.

Anteriormente à Lei do Cibercrime, o legislador descurou as especiais particularidades da prova em formato eletrónico e remeteu-a para o regime da interceção e gravação das comunicações telefónicas, o que se justifica quanto à interceção e registo das comunicações, uma vez que estamos no domínio das telecomunicações apenas com a destrinça do meio utilizado sobre qual incide a diligência, contudo esta razão não se justifica quanto às comunicações que se encontram armazenadas.

Apesar da Lei do Cibercrime ter seguido esta mesma orientação e não ter feito uma revogação expressa do regime geral previsto no art.º 189º, as questões que suscitaram não só na doutrina, como também na jurisprudência foram sobretudo quanto à relação entre a Lei 109/2009 e o art.º 189º do CPP.

A Lei 109/2009, procurou adaptar o regime de meios de obtenção de prova à prova digital e procedeu à previsão de um regime plasmado para a interceção da comunicação assim como, um regime para os dados resultantes dessa mesma comunicação.

Quanto ao primeiro, como mencionado ao longo da dissertação, encontra-se previsto no art.º 18º e não foge muito ao que se encontra previsto no regime geral, nem faria sentido, uma vez que é objeto da mesma tutela e também porque estamos perante uma interceção em tempo real da comunicação.

Todavia, quanto ao regime previsto para os dados armazenados, ou seja, os dados que resultam da comunicação, o legislador, no art.º 17º da Lei 109/2009, remeteu para o regime da apreensão da correspondência previsto no regime geral, que no nosso entendimento deveria ser remetido para o regime geral das buscas previsto no art.º 174º e segs. do CPP, uma vez que deixamos de estar perante uma comunicação e passamos a estar perante um mero escrito em suporte digital.

Apesar de não haver uma revogação expressa do art.º 189º, entendemos que o mesmo deixa de ter aplicação prática sempre que estejamos perante questões de recolha de prova em formato digital, passando a mesma a reger-se pelo regime previsto no art.º 18 da Lei 109/2009.

Quando estamos perante uma ingerência em comunicações armazenadas em suporte digital e acesso a dados que se encontrem em formato digital, a lei que constitui referência é a Lei 109/2009 nos seus artigos 12º a 17º, deixando o art.º 189º de ter aplicação neste campo.

Posto isto, é de ressalvar que a prova digital é uma realidade com cada vez mais relevância fruto da utilização genérica destes meios, assim uma regulação dispersa em vários diplomas apenas contribui para o surgimento de zonas cinzentas suscetíveis de duvidas e consequentemente uma má aplicação pelos órgãos judiciais. Tal como JOÃO

CONDE CORREIA[48] afirma *"a qualidade da lei vigente é condição essencial para a qualidade do direito quotidianamente aplicado: sem uma boa lei, por melhores que sejam os nossos juristas, dificilmente haverá bom direito"*.

A descentralização normativa da matéria da prova digital pode revelar-se perniciosa para um sistema jurídico coerente, a Lei 32/2008 e a Lei 109/2009 são exemplo disso, ao invés de termos o regime da prova digital previsto num único diploma, esta para além de não dar resposta a todas as questões, encontra-se disposta em três diplomas distintos.

Ao invés desta descentralização, o desejável seria um sistema unificado e claro *"um corpo legislativo integrado, coerente e uniforme, capaz de satisfazer as necessidades práticas e de salvaguardar o desejável nível ideal de proteção dos direitos individuais"*[49].

Desta feita, concluímos que a legislação prevista para a obtenção de prova digital revela alguns defeitos, sobretudo na falta de capacidade de responder às novas realidades que urgem soluções. O legislador deverá centralizar e clarificar o regime previsto para a prova digital.

[48] JOÃO CONDE CORREIA, *"Prova digital: as leis que temos e a lei que devíamos ter"*, (…) *ob.cit.* pág. 52 e ss.
[49] JOÃO CONDE CORREIA, (…) *ob.cit.* pág. 52 e ss.

Bibliografia

1. 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"*, Universidade Católica Editora, 2008;

2. ANDRADE, MANUEL DA COSTA, *"Bruscamente no verão passado, a Reforma do Código de Processo Penal-Observação críticas sobre uma lei que podia e devia ter sido diferente",* Coimbra Editora, 2009;

3. MILITÃO, RENATO LOPES, *"A Propósito da Prova Digital"*, consultável em: http://www.oa.pt/upl/%7B53f46e96-536f-47bc-919d-525a494e9618%7D.pdf;

4. CASABONA, CARLOS MARIA ROMEO, *"La protección penal de los mensajes de correo electrónico y de otras comunicaciones de catácter personal a través de internet"*, consultável em: https://www.unifr.ch/ddp1/derechopenal/obrasportales/op_20080612_17.pdf

5. RAMOS, ARMANDO DIAS, *"A prova digital em Processo Penal: o correio eletrónico"*, Chiado Editora, 1ª edição, Novembro de 2014;

6. MESQUITA, PAULO DÁ, *"Processo Penal, Prova e Sistema Judiciário*", Coimbra Editora, 2010;

7. NEVES, RITA CASTANHEIRA, *"As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova",* Coimbra Editora, 2011;

8. RODRIGUES, BENJAMIM SILVA, *"das escutas telefónicas - A monitorização dos fluxos informacionais e comunicacionais, Tomo I"*, Coimbra Editora, 2008;

9. VERDELHO, PEDRO, *"Apreensão de Correio Eletrónico em Processo Penal"*, in Revista do Ministério Público, Ano 25.º, 2004;

10. TEIXEIRA, CARLOS ADÉRITO, Revista do CEJ (nº9), 1º semestre 2008;

11. GONÇALVES, FERNANDO; ALVES, MANUEL, *"Crime. Medidas de Coação e Prova",* Almedina, 2015;

12. JESUS, FRANCISCO MARCOLINO DE,*"Os Meios de Obtenção da Prova em Processo Penal,* Almedina, 2ª Edição, 2015.

Acórdãos

1. Acórdão do Tribunal da Relação de Évora, de 07 de Abril de 2015, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/ad8068a8c8f9b3c080257e2e00356d33?OpenDocument&Highlight=0,189%C2%BA,CPP ;

2. Acórdão do Tribunal da Relação de Guimarães, de 15 de Outubro de 2012, disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/d7e67584752588c980257aa0004607bc?OpenDocument ;

3. Acórdão do Tribunal da Relação de Évora, de 20 de Janeiro de 2015, disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument ;

4. Acórdão do Tribunal da Relação do Porto, de 20 de Janeiro de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/54a82f139588437f80257f5a0033e764?OpenDocument&Highlight=0,189%C2%BA,CPP ;

5. Acórdão do Tribunal da Relação do Porto, de 13 Abril de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument&Highlight=0,109%2F2009;

Siglas e Abreviaturas

Art.º- Artigo;
CPP- Código de Processo Penal;
CRP- Constituição da República Portuguesa;
Cfr. – Confrontar;
Ex vi – Por força de;
Ob. Cit.- Obra citada;
Pág.- Página;
SS- Seguintes;
Vol.- Volume.

Índice