Mestrado Forense

OS MEIOS DE OBTENÇÃO DE PROVA NA LEI DO CIBERCRIME E O SEU CONFRONTO COM O CÓDIGO DE PROCESSO PENAL

Dissertação de Mestrado apresentada à Universidade Católica Portuguesa para obtenção de grau de Mestre por Maria Joana Xara-Brasil Marques, sob orientação do Professor Doutor Henrique Salinas.

UNIVERSIDADE CATÓLICA PORTUGUESA

Lisboa, 01 de Julho de 2014

I
INTRODUÇÃO[1]

É incontestável o papel que as Novas Tecnologias da Informação e da Comunicação - nomeadamente a Internet – têm quer na vida dos cidadãos, das empresas como até do próprio Estado, que apoia na Internet "as suas tradicionais funções."[2]

A par dos efeitos positivos que a expansão das redes de comunicação proporcionou, propiciou igualmente o aparecimento de um novo tipo de criminalidade: a cibercriminalidade ou criminalidade informática. Trata-se de uma realidade bastante complexa, principalmente pelo facto de se situar num espaço não físico, ou seja, num espaço virtual, digital.

Desde logo, a criminalidade informática pode ser entendida sob dois prismas diferentes: por um lado, pode ser considerada num sentido amplo, englobando todos os ilícitos criminais praticados através de meios informáticos, ou, num sentido mais restrito, englobando apenas os crimes cujo tipo legal pressupõe a prática de uma conduta criminosa através do uso de meios informáticos ou contra um bem informático.

Apesar de se tratar de uma realidade relativamente recente, a mesma não é desconhecida para o legislador português. Já em 1991, vigorava no ordenamento jurídico português a Lei nº 109/91, de 17 de Agosto - também denominada "Lei da Criminalidade Informática" – destinada a prevenir e combater este tipo de criminalidade.

No entanto, embora contemplasse um conjunto de ilícitos criminais, não se encontrava previsto um regime jurídico de recolha de prova em ambiente digital.

Estamos perante uma realidade de natureza digital. Ora, para combater este tipo de criminalidade, em qualquer uma das suas acepções, não basta criminalizar um conjunto de actos, sendo absolutamente indispensável providenciar às autoridades criminais os meios e instrumentos, que os auxiliem na investigação e no combate contra este tipo de crimes. As tradicionais buscas, apreensões, revistas, ou seja, os tradicionais meios de obtenção de prova, encontravam-se vocacionados para um ambiente físico – e não para um ambiente digital.

[1] O presente texto não foi redigido ao abrigo do Novo Acordo Ortográfico.
[2] Exposição dos Motivos da Proposta de Lei nº 289/X/4ª – Lei da Cibercriminalidade.

E, tal como referia Paulo Dá Mesquita, até 2009, existia a necessidade de se proceder a uma "reconstrução conceptual complexa, com um enquadramento teórico que se adaptasse à rotura epistemológica introduzida pelas novas tecnologias no processamento, captação e memória das comunicações."[3]

E, embora a nível internacional esta preocupação tivesse sido atendida – com a realização da Convenção sobre o Cibercrime, que contemplou um conjunto de mecanismos processuais especificamente destinados a garantir e regular o modo de obtenção da chamada "prova digital" - em Portugal, essas medidas só viriam a ser implementadas em 2009 (embora Portugal tivesse assinado a Convenção em 2001…).

Desta forma, até 2009 (ano da entrada em vigor da Lei do Cibercrime), só era possível proceder à recolha de prova em ambiente digital nos termos definidos pelos artigos 187.º e seguintes do Código de Processo Penal, por força da remissão legal contemplada no artigo 189.º número 1.

Assim, para que as autoridades criminais pudessem proceder à recolha da chamada "prova digital", quer por via da intercepção de comunicações electrónicas, quer por via da ingerência nas comunicações electrónicas armazenadas em suporte digital, teriam de estar reunidos os pressupostos e requisitos previstos nos artigos 187.º e seguintes do Código de Processo Penal.

Os artigos 187.º e seguintes do Código de Processo Penal regulam a intercepção e gravação de comunicações telefónicas. Estamos perante um meio de obtenção de prova - também conhecido por "escutas telefónicas" – que, devido ao seu carácter bastante intrusivo, tem um âmbito de aplicação bastante restrito, só sendo possível recorrer ao mesmo em processos relativos ao elenco de crimes previstos no artigo 187.º número 1.

Efectivamente, até à entrada em vigor da Lei do Cibercrime, era possível proceder à recolha de prova digital.

No entanto, o carácter restritivo do regime da intercepção e gravação de comunicações telefónicas, dificultava o curso das investigações, e inclusive, em alguns casos, até a subsistência das próprias investigações, que muitas vezes chegavam a um impasse e encontravam sérios obstáculos processuais.

[3] Paulo Dá Mesquita, *Processo Penal, Prova e Sistema Judiciário,* Coimbra Editora, 2011, pp. 84 e 85.

E, sendo a recolha de prova em ambiente digital absolutamente imprescindível na investigação dos chamados "crimes informáticos" - e, em muitos casos, a única existente – em muitos desses crimes, por não serem subsumíveis ao elenco de crimes previstos no artigo 187.º número 1 do Código de Processo Penal, a recolha de prova digital não era admissível.

A Lei do Cibercrime veio, desta forma, colmatar uma lacuna que existia, há muito, no sistema processual penal português, providenciando aos órgãos de polícia criminal os meios necessários, não só para o combate dos crimes previstos na respectiva lei – os chamados "cibercrimes" - como também para garantir o combate contra a criminalidade informática em geral.

No entanto, tendo a Lei do Cibercrime contemplado, pela primeira vez no ordenamento jurídico português, um regime específico e detalhado de recolha da prova em ambiente digital, e não tendo revogado expressamente o artigo 189.º número 1 do Código de Processo Penal (que determina a aplicação do regime das "escutas telefónicas" quer à intercepção e registo de comunicações electrónicas, quer às comunicações electrónicas armazenadas em suporte digital), coloca-se a questão de saber como conciliar as várias disposições processuais relativas à obtenção da prova digital.

Estaremos perante um conflito de disposições processuais? Ou por sua vez, disposições processuais que se poderão complementar entre si? Este é o objecto da presente Dissertação.

Assim, a presente exposição tem como propósito procurar - depois de uma cuidada análise ao conjunto dos meios de obtenção de prova digital previstos na Lei do Cibercrime - chegar a uma solução processual, sobre o modo de articulação das várias disposições processuais, de modo a facilitar o trabalho das autoridades criminais e garantir um combate eficaz contra a criminalidade informática (aqui entendida num sentido lato).

II
FONTES NORMATIVAS INTERNACIONAIS NO ÂMBITO DA CIBECRIMINALIDADE

Antes de se partir para a análise das disposições processuais previstas na Lei do Cibercrime, cumpre enquadrar a mesma, quer no plano nacional, quer no plano internacional.

Dada a natureza que reveste a cibercriminalidade, pode ser considerado como dado adquirido, que estamos perante uma realidade transfronteiriça.

E, partindo desta premissa, não basta que as legislações nacionais criem, isoladamente, mecanismos legais destinados a prevenir e garantir o combate contra a cibercriminalidade.

Ao invés, devem ser criados instrumentos legais, de carácter universal e de cooperação internacional, de modo a poderem vir a ser implementados por todos os Estados. Só assim o combate contra a cibercriminalidade será eficaz.

Embora existam múltiplos diplomas e trabalhos internacionais a respeito da cibercriminalidade e da prova digital, destacam-se três diplomas, pelo impacto que tiveram na legislação portuguesa:

2.1 Convenção sobre o Cibercrime do Conselho da Europa, de 23 de Novembro de 2001;
2.2 Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro;
2.3 Directiva nº 2006/24/CE, do Parlamento e do Conselho, de 15 de Julho.

2.1 Convenção sobre o Cibercrime do Conselho da Europa, de 23 de Novembro de 2001

Estamos perante um dos instrumentos legislativos que serviu de modelo para a Lei nº 109/2009, de 15 de Setembro, mais conhecida por "Lei do Cibercrime".

Partindo da premissa do carácter universal e transfronteiriço da cibercrminalidade, em 23 de Novembro de 2001 foi aprovada, em Budapeste, pelo Conselho da Europa a Convenção sobre o Cibercrime.

A Convenção sobre o Cibercrime é considerada "o primeiro e mais importante trabalho internacional de fundo sobre crime no ciberespaço."[4]

A Convenção sobre o Cibercrime teve como objectivo criar mecanismos destinados a "proteger a sociedade contra a criminalidade no ciberespaço, designadamente através da adopção de legislação adequada e da melhoria da cooperação internacional."[5]

Tendo presente o carácter transfronteiriço inerente à criminalidade informática, a Convenção procurou, através da previsão de normas penais materiais, processuais e de cooperação internacional, harmonizar as várias legislações dos países signatários, promovendo, desta maneira, um combate mais eficaz contra a cibercriminalidade.

A Convenção sobre o Cibercrime contemplou:

1. Um conjunto de conceitos informático-jurídicos;
2. Um conjunto de ilícitos criminais;
3. Um conjunto de medidas processuais destinadas a regular a forma de obtenção de prova em ambiente digital e,
4. Mecanismos destinados a promover a cooperação internacional.

A Convenção fixou igualmente, regras de aplicação espacial dos crimes previstos na mesma.

Portugal subscreveu a Convenção sobre o Cibercrime em 2001.

No entanto, só procedeu à sua ratificação em 2009, por Resolução da Assembleia da República nº 88/2009 e pelo Decreto do Presidente da República nº 92/2009, ambos publicados a 15 de Setembro (data da publicação da Lei nº 109/2009, de 15 de Setembro).

A Lei nº 109/2009, de 15 de Setembro, como consta no próprio texto, adaptou ao direito interno a Convenção sobre o Cibercrime. Por este facto e pelo papel que teve e que continua a ter no combate contra a cibercriminalidade, era essencial mencioná-la na presente exposição.

[4] Exposição dos Motivos da Proposta de Lei nº 289/X/4ª – Lei do Cibercrime.
[5] Preâmbulo da Convenção sobre o Cibercrime.

A par da Convenção sobre o Cibercrime, que serviu de modelo para a Lei do Cibercrime, destacam-se ainda outro diploma legal: a **Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro.**

2.2 Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro

Deve igualmente ser mencionada na presente exposição a Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro por se tratar de um importante diploma comunitário em matéria de cibercriminalidade e por ter sido transposta para o ordenamento jurídico português através da Lei nº 109/2009, de 15 de Setembro.

A Decisão-Quadro nº 2005/222/JAI do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas informáticos, acompanhou as linhas orientadoras promovidas pela Convenção sobre o Cibercrime.

Tal como a Convenção, a Decisão-Quadro teve como objectivo "reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes (…) mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação."[6], tendo em atenção que "a natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio."[7]

2.3 A Directiva nº 2006/24/CE, do Parlamento e do Conselho de 17 de Julho

A Directiva supra citada, reporta-se à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou em redes públicas de comunicações.

A respectiva Directiva foi transposta para a ordem jurídica portuguesa através da Lei nº 32/2008, de 17 de Julho

[6] Ponto (1) da Decisão-Quadro nº 2005/222/JAI do Conselho, de 24 de Fevereiro.
[7] Ponto (5) da Decisão-Quadro nº 2005/222/JAI do Conselho, de 24 de Fevereiro.

III
EVOLUÇÃO LEGISLATIVA DO REGIME DE OBTENÇÃO DA PROVA DIGITAL NO SISTEMA PROCESSUAL PENAL PORTUGUÊS

Até 2009, encontra-se em vigor a Lei da Criminalidade Informática, criada com o objeco de combater a criminalidade informática.

Estando em vigor desde 1991, a Lei da Criminalidade Informática revelou-se, com o decorrer dos tempos, desadequada e desactualizada face ao desenvolvimento e aparecimento de novas formas de actuação criminosa no ciberespaço.

Estávamos perante um diploma legal que "adequado à realidade que se destinava a regular na data em que entrou em vigor, pelo decurso de quase duas décadas, tornou-se deficitário."[8]

E, embora a Lei do Cibercrime tivesse revogado a Lei da Criminalidade Informática[9], a verdade é que manteve algumas normas penais materiais (que já se encontravam contemplas na Lei da Criminalidade Informática), acabando somente por remodelar e adequar o ordenamento jurídico português às exigências internacionais e nacionais.

Embora contemplasse um conjunto de mecanismos com vista a combater a cibercriminalidade, não se encontrava contemplado na Lei da Criminalidade Informática um regime jurídico de obtenção da prova digital.

Assim, até 2009 - data da entrada em vigor da Lei do Cibercrime - não estava previsto no direito processual penal português um regime que regulasse, de forma específica e detalhada o modo de obtenção da prova digital.

Ao invés, na Alemanha, a obtenção de prova electrónica já se encontrava regulada desde 1968, através da Lei de Restrição do Segredo Postal, de Correspondência e das Comunicações à Distância e do Código de Processo Penal alemão.

Actualmente, no Capítulo VIII, do Código de Processo Penal alemão, encontram-se regulados os meios de obtenção de prova, incluindo-se a apreensão de correspondência virtual, intercepção de telecomunicações e buscas em computadores, enncontrando-se

[8] Exposição dos Motivos da Proposta de Lei nº 289/X/4ª – Lei da Cibercriminalidade.
[9] Artigo 31.º da Lei nº 109/2009, de 15 de Setembro, que aprovou a Lei do Cibercrime.

previstos no § 100 a. e b., os pressupostos e requisitos da intercepção e gravação de telecomunicações.

Regressando ao ordenamento jurídico português, não se pode dizer de uma forma absoluta que não existia nenhuma norma que regulasse o modo de recolha da prova digital. Existia. Mas a recolha de prova digital era admitida de uma forma (bastante) restrita.

A recolha de prova em ambiente digital já se encontra regulada no Código de Processo Penal desde a década de 90.

Na versão originária do Código de Processo Penal de 1987, encontrava-se consagrada no artigo 190.º uma extensão legal do regime da intercepção e gravação de comunicações telefónicas – as conhecidas "escutas telefónicas" – "às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone."

A redacção deste preceito levantou um conjunto de dúvidas no seio da doutrina e da jurisprudência, quanto ao alcance da expressão "meio técnico diferente do telefone". Estas dúvidas viriam a ser esclarecidas com a nova redacção dada ao artigo 190.º pela Lei nº 59/98, de 25 de Agosto.

Em 1998, com a Revisão do Código de Processo Penal, foi estendida a aplicação do regime das "escutas telefónicas" a comunicações à distância "de um conjunto de serviços informáticos fornecidos através de uma rede de telecomunicações."[10]

Em 2007, com a Revisão do Código de Processo Penal – através da Lei nº 48/2007, de 29 de Agosto - o legislador procedeu à ampliação do artigo 190.º (actual 189.º) estendendo a aplicação do regime das "escutas telefónicas às comunicações ou conversações electrónicas (ou seja, dados informáticos) armazenadas em suporte digital.

Assim, o anterior artigo 190.º passou a ter a seguinte redacção: "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 electrónico ou outras formas de transmissão de dados por via telemática, bem como à intercepção das comunicações entre presentes."

[10] Paulo Dá Mesquita, op.cit. p. 102.

A Reforma de 2007 manteve inalterada "a sistematização original de 1987,"[11] relativa ao regime das "escutas telefónicas como sendo o "quadro global da regulação da intercepção e registo de telecomunicações."[12]

A ampliação levada a cabo pelo legislador foi objecto de duras críticas por parte da doutrina e jurisprudência.[13]

Tal como refere Paulo Dá Mesquita, assistiu-se a uma "grave lacuna num processo de reforma[14]", porquanto, para o Autor, as alterações trazidas pelo legislador no campo da prova digital revelaram a "ausência de um pensamento conceptualmente exigente sobre a teleologia e semântica dos institutos probatórios em face da evolução tecnológica e a sua repercussão na interacção comunicacional e registos de dados."[15]

Mais, para além desta crítica, pode ser invocado igualmente que o legislador não teve qualquer tipo de respeito pelas exigências internacionais, exigências estas a que o Estado português se encontrava adstrito.

Como Faria Costa menciona, "a elaboração da respectiva proposta" (que esteve na base da Lei nº 48/2007, de 29 de Agosto) exigia "um labor e um rigor científicos, que visivelmente, não precederam a proposta em análise."[16]

Os Acórdãos dos Tribunais da Relação de Guimarães, de 12 de Outubro de 2009[17], e da Relação do Porto de 27 de Janeiro de 2010[18], entre outros[19], são exemplos das inúmeras críticas tecidas a propósito da ampliação levada a cabo pelo legislador em 2007, tendo os mesmos feito uma interpretação *contra legem* do preceito em questão, recusando a aplicação do artigo 189.º número 1, segunda parte, quando estivesse em causa a

[11] Paulo Dá Mesquia, op. cit. p. 89.
[12] Paulo Dá Mesquita, op. cit. p. 89.
[13] Em sentido contrário: Fernanda Palma, que defendia que o simples facto de a acto comunicacional ter terminado não justificava a cessação da protecção legal "decorrente da aplicação do procedimento previsto para as escutas"
[14] Paulo Dá Mesquita, op. cit. p. 88.
[15] Paulo Dá Mesquita, op. cit. p. 88.
[16] Paulo Dá Mesquita, op. cit. p.88.
[17] Proc. n.º 1396/08.1PBGMR – A.G1 – consultável em: www.dgsi.pt.
[18] Proc. n.º 896/07.5JAPRT.P1 – consultável em: www.dgsi.pt.
[19] Também seguiram esta linha de entendimento: , cfr. Acs. da Rel. de Coimbra, de 29/03/2006, proc. n.º 607/06; da Rel. de Lisboa de 20/03/2007, proc. n.º 7189/2006 – 7, e de 15/07/2008, proc. n.º 3453/2008, consultável em www.dgsi.pt.

apreensão de mensagens de telefone – as "SMS'S" - já recebidas/lidas e armazenadas pelo destinatário, equiparando-as ao arquivo físico recebido, lido e guardado.

Deste modo, até 2009, a única disposição legal que previa a admissibilidade da recolha de prova digital, era o artigo 189.º número 1 do Código de Processo Penal, que remetia para a aplicação do regime das "escutas telefónicas", regime este regulado pelos artigos 187.º e seguintes.

Esta disposição processual acabava por limitar e gerar um verdadeiro obstáculo processual na investigação de determinados crimes - os "crimes informáticos".

Isto porque, dado o carácter bastante restrito de admissibilidade de utilização desta diligência - só sendo possível a sua utilização em processos relativos aos crimes previstos no artigo 187.º número 1 do Código de Processo Penal – impedia a recolha de prova digital em processos onde a recolha deste tipo de prova era absolutamente essencial (e em alguns casos, o único tipo de prova existente).

Temos o caso, por exemplo, do crime de *reprodução ilegítima de programa protegido* (actual artigo 8.º da Lei do Cibercrime) que se encontrava previsto na (agora revogada) Lei da Criminalidade Informática, em que não era permitida a recolha de prova digital nos termos dos artigos 187.º e seguintes do Código de Processo Penal uma vez que não se encontrava preenchido o requisito legal do artigo 187.º número 1, nomeadamente, por prever uma pena de prisão aplicável, até três anos.

Só em 2003 é que foi apresentado, na Assembleia da República, o Projecto de Lei nº 217/X, de 27 de Janeiro, que propôs a criação de um regime jurídico de recolha da prova digital.

No seguimento deste Projeto de Lei, foi apresentada uma Proposta de Lei, em 2004 pelo Governo. No entanto, a Proposta de Lei nunca chegou a ser discutido em Conselho de Ministros.

É de realçar que Portugal assinou a Convenção sobre o Cibercrime em 2001. No entanto, só procedeu à sua ratificação em 2009, passado oito anos..

Ao invés, no ordenamento jurídico italiano, a ratificação da respectiva Convenção ocorreu em 2008, através da aprovação da "Legge 18 marzo 2008, n. 48".

No caso português, só em 2009, com a aprovação da Lei do Cibercrime, viria a ser introduzido, pela primeira vez no ordenamento jurídico português, um regime jurídico de recolha da prova digital.

IV

A LEI Nº 109/2009, DE 15 DE SETEMBRO – A "LEI DO CIBERCRIME"

4.1 Notas Preliminares

Até 2009, Portugal ainda não tinha dado cumprimento às obrigações internacionais a que se encontrava adstrito (não esquecer que Portugal já tinha assinado a Convenção sobre o Cibercrime em 23 de Novembro de 2001…).

Tal facto só viria a concretizar-se em 2009, com a publicação da Lei nº 109/2009, de 15 de Setembro também denominada "Lei do Cibercrime", tendo a mesma entrado em vigor em Outubro de 2009.

Em 15 de Setembro de 2009, Portugal procedeu, igualmente, à ratificação da Convenção sobre o Cibercrime[20], e do Protocolo Adicional à Convenção sobre o Cibercrime, relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos.

A Lei do Cibercrime transpôs para a ordem jurídica portuguesa a Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistema de informação e adaptou o direito interno à Convenção sobre o Cibercrime.

Conforme consta da Exposição de Motivos da Proposta de Lei nº 289/X/4ª (que serviu de base ao texto da Lei do Cibercrime), em vez de se ter procedido a uma alteração das diversas fontes normativas relativas a este tipo de criminalidade, optou-se por englobar num só diploma legal todas as disposições – penais materiais, processuais e de cooperação internacional – relativas ao sector da cibercriminalidade, por ser a solução que se mais se coaduna com a "tradição portuguesa"[21].

Paulo Dá Mesquita defendia, ao invés, "a integração das regras no Código de Processo Penal,"[22] tal como se observou no ordenamento jurídico italiano, onde o legislador, em vez de ter procedido à criação de um regime jurídico autónomo e específico para a recolha de prova em ambiente electrónico, acabou por proceder a um conjunto de alterações no seio do Código de Processo Penal, tendo sido acrescentadas disposições

[20] Ponto 1.1 da presente Dissertação.
[21] Exposição dos Motivos da Proposta de Lei nº 289/X/4ª .
[22] Paulo Dá Mesquita, ob. cit. p. 101.

processuais relativas à forma de obtenção de prova electrónica, adaptando assim os tradicionais meios de obtenção de prova à prova em ambiente digital.

Ao invés, o legislador português - tal como o legislador alemão - englobou num único diploma legal o conjunto das disposições jurídicas relativas à cibercriminalidade.

No entanto, o legislador alemão tem vindo ao longo do tempo, como refere Manuel da Costa Andrade, a "erigir um regime unificado e sistematizado dos meios ocultos de investigação e assegurar o respeito, neste domínio, da área nuclear inviolável da intimidade."[23], criando um verdadeiro sistema, não deixando os meios ocultos de investigação serem regulados em leis extravagantes.

Em comparação com o ordenamento jurídico português, a lei processual penal alemã acaba por ir mais longe do que a portuguesa, admitindo o uso de meios ocultos de investigação mesmo que representem um maior grau de lesividade, permitindo por exemplo, o recurso às *buscas online* quando se verifique indícios de um "perigo concreto para a vida, a integridade física ou a liberdade da pessoa ou para bens da comunidade cuja ameaça afecte as bases, a existência ou os fundamentos da existência do Homem."[24]

Por sua vez, no ordenamento jurídico espanhol, o legislador optou por regulamentar num só artigo - o artigo 579.º da "Ley de Enjuiciamento Criminal" – o regime de recolha da prova em ambiente digital (apreensão de correspondência, intercepção de comunicações, escutas telefónicas).[25]

Retomando agora a análise da Lei do Cibercrime, esta contempla um conjunto de disposições penais materiais, processuais e de cooperação internacional.

---

[23] Manuel da Costa Andrade, "*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, p. 24.

[24] Rita Castanheira Neves, op. cit. p. 104.

[25] Quanto ao artigo 579.º tem sido levantada a questão da (in)constitucionalidade do referido artigo, por violação do artigo 18.º número 3 (direito ao segredo das comunicações) da Constituição espanhola, pelo facto de a norma não ser "suficientemente desenvolvida ou determinada", não "cumprindo o requisito do *quality of the law*, exigido pelo Tribunal Europeu dos Direitos do Homem."[25] No entanto, Tribunal Constitucional espanhol tem-se dividido sobre qual a solução a seguir.

Como foi anteriormente referido[26], a Convenção sobre o Cibercrime, teve como principal objectivo "proteger a sociedade do cibercrime, nomeadamente através da adopção de legislação adequada e do fomento da cooperação internacional."[27]

A Convenção estabeleceu um conjunto de disposições penais materiais, processuais e normas destinadas a promover a cooperação internacional. E, tendo Portugal assinado e procedido à sua ratificação, "o acolhimento das obrigações legislativas decorrentes da Convenção" impôs "também a alteração do regime (…) vigente (à data).[28] [29]"

A verdade é que, embora a Lei do Cibercrime tivesse procedido à revogação da Lei da Criminalidade Informática (artigo 31.º) no que respeita ao direito penal material, verificou-se "apenas ajustamentos da (…) legislação sobre criminalidade informática[30]". Neste ponto, a Lei do Cibercrime limitou-se a proceder a uma remodelação de conceitos jurídico-informáticos, acabando também por introduzir novos tipos de ilícitos criminais.

4.2 O carácter inovador da Lei nº 109/2009, de 15 de Setembro

Já do ponto de vista processual, a questão é diversa. A Lei do Cibercrime foi o primeiro diploma legal a contemplar na ordem jurídica portuguesa, um regime específico de obtenção da prova digital. É daqui que advém carácter inovador desta lei.

Como referido no Acórdão da Relação de Lisboa, de 22 de Janeiro de 2013[31], a Lei do Cibercrime, ao prever um regime jurídico específico para a recolha de prova digital, acabou por "superar a lacuna da Lei nº 109/91 de 17 de Agosto (Criminalidade Informática) que, por não conter essas normas processuais que adequassem o regime legal às particularidades da investigação "empurrou" a jurisprudência para a interpretação de que só em relação a crimes de catálogo seria possível a obtenção de certo tipo de dados como os dados de tráfego e mercê da intervenção do juiz de instrução."[32]

Contemplou igualmente mecanismos destinados a promover a cooperação internacional.

[26] Ponto 2.1 da presente Dissertação.
[27] Preâmbulo da Convenção.
[28] Exposição dos Motivos da Proposta de Lei nº 289/X/4ª – Lei da Cibercriminalidade.
[29] Até 2009, encontrava-se em vigor a Lei da Criminalidade Informática.
[30] Exposição dos Motivos da Proposta de Lei nº 289/X/4ª – Lei da Cibercriminalidade.
[31] Disponível em: www.dgsi.pt.
[32] Disponível em: www.dgsi.pt

Conforme consta da Exposição de Motivos, dado o carácter deficitário do sistema processual penal português em matéria de obtenção da prova digital, era urgente, "superar o actual (até 2009) regime, de modo a fornecer ao sistema processual penal normas que permitissem a obtenção de dados de tráfego e a realização de intercepções de comunicações em investigações de crimes praticados no ambiente virtual.[33]"

A Lei do Cibercrime apresentou-se, deste modo, como uma forma de colmatar uma lacuna que existia, há muito tempo, no sistema processual penal português.

Tal como refere Paulo Dá Mesquita, "a adaptação do direito português à Convenção sobre o Cibercrime do Conselho da Europa (…) implicava que se alterasse o restritivo regime consagrado pelo artigo 189.º número 1 do Código de Processo Penal."[34]

E mais, veio introduzir um regime processual não aplicável somente a processos relativos a crimes previstos na respectiva lei, como também a processos relativos a crimes cometidos através de um sistema informático ou em qualquer processo criminal em que seja necessário proceder a recolha da chamada prova digital. É o que dispõe o artigo 11.º da referida Lei, que será analisado posteriormente.

Assim, a Lei do Cibercrime veio, do ponto de vista processual, contemplar um conjunto de meios de obtenção de prova, direcionados para o ambiente digital. Como se verá adiante, muitos destes meios de obtenção de prova digital acabam por ser uma adaptação dos tradicionais meios de obtenção de prova previstos no Código de Processo Penal (mas adaptados ao ambiente digital).

Assim, como indica Pedro Verdelho, o aparecimento desta lei propiciou o aparecimento de "novas ferramentas processuais".[35]

[33] Cf. Exposição dos Motivos da Proposta de Lei nº 289/X/4ª – Lei da Cibercriminalidade.
[34] Paulo Dá Mesquita, op. cit. p. 102.
[35] Entrevista de Pedro Verdelho ao Jornal de Notícias, em 21 de Janeiro de 2010.

V
ANÁLISE DOS MEIOS DE OBTENÇÃO DE PROVA PREVISTOS NA LEI DO CIBERCRIME

Feito o devido enquadramento e não sendo possível analisar com exaustão todas as disposições legais previstas na Lei do Cibercrime, cumpre analisar neste momento, as disposições processuais que se encontram previstas na respectiva lei.

Como já foi referido, o carácter inovador da Lei do Cibercrime não advém propriamente das disposições penais materiais nela previstas, mas sim das disposições processuais previstas no Capítulo III.

Isto deve-se ao facto de a Lei do Cibercrime ter sido o primeiro diploma legal a prever um regime jurídico de obtenção de prova em ambiente digital. E um regime jurídico não aplicável somente a processos relativos aos crimes previstos na respectiva lei.

5.1. Âmbito de aplicação das disposições processuais

O artigo 11.º estabelece o âmbito material de aplicação das disposições processuais previstas no Capítulo III.

Servindo a Convenção sobre o Cibercrime de modelo da Lei nº109/2009, o artigo 11.º encontra correspondência no artigo 14.º da referida Convenção.

Pode ser afirmado que as medidas processuais de recolha da prova digital, previstas na Lei do Cibercrime, têm como Pedro Venâncio refere, um campo "de aplicação geral", na medida em que estamos perante a possibilidade de recurso a estes "meios de obtenção de provas digitais para o combate da criminalidade, seja qual for a sua forma." [36]

Estamos assim, perante um regime processual de obtenção da prova digital com um campo de aplicação mais abrangente do que a própria Lei, não restringindo a sua utilização apenas a processos relativos aos crimes nela contemplados, mas também:

[36] Pedro Venâncio, "JusJornal" N.º 1182, 23 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer.

1. A crimes praticados através de um sistema informático, ou
2. Em processos relativos a crimes em que, independentemente da natureza ou moldura penal do crime, seja necessário, no decurso da investigação criminal, proceder à recolha de prova digital.

Isto porque, o que se pretende efectivamente com a criação deste regime de recolha de prova digital é de providenciar às autoridades criminais, instrumentos que permitam o combate contra a criminalidade em geral e não apenas relativa aos crimes previstos na Lei do Cibercrime. Temos que ter presente que os meios informáticos podem ser utilizados como instrumentos para a prática de um conjunto indeterminável de crimes.

E o artigo 11.º ao permitir a utilização dos meios de obtenção de prova em processos relativos a um conjunto indeterminável de crimes, acabou por disponibilizar um conjunto de instrumentos processuais, que há muito vinham a ser reclamados e exigidos pelas autoridades criminais, não só para combater a criminalidade informática, em sentido restrito, mas da criminalidade informática em geral.

Desta maneira, estamos perante o aparecimento de um regime, de carácter geral ou seja, não apenas aplicável aos crimes previstos na Lei do Cibercrime.

Assim, de acordo com o estatuído no artigo 11.º, podemos concluir que os meios de obtenção de prova previstos nos artigos 12.º a 17.º são de aplicação geral, ou seja, podem ser utilizados em processos relativos aos crimes previstos na respectiva lei, mas não só.

No entanto, o artigo 11.º excepciona a aplicabilidade dos artigos 18.º e 19.º a um número indiscriminado de crimes, tendo estes dois artigos um âmbito de aplicação bastante mais restrito que os demais meios de obtenção de prova previstos no Capítulo III. Tal excepção justifica-se pelo carácter bastante intrusivo destas duas diligências.

Por outro lado, número 2 do artigo 11.º alerta que as disposições processuais previstas na Lei do Cibercrime "não prejudicam o regime da Lei nº 32/2008, de 17 de Julho."

A Lei nº 32/2008, de 17 de Julho transpôs para a ordem jurídica portuguesa, a Directiva nº 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de

comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

Como refere Rita Castanheira Neves, "a Lei do Cibercrime tem um âmbito de aplicação delineado, não se podendo "perder de vista os requisitos da Lei nº 32/2008, de 17 de Julho."[37]

Mais, para a Autora, face ao disposto no artigo 11.º número 2, "somos forçados a demarcar campos de aplicação distintos para a Lei do Cibercrime e para a Lei nº 32/2008, de 17 de Julho"[38], aplicando-se esta última lei à investigação dos chamados "crimes graves" (terrorismo, criminalidade altamente organizada), definidos no artigo 2.º número 1 alínea g).

Assim, para Rita Castanheira, quando esteja em causa a investigação deste tipo de criminalidade, a obtenção de dados de tráfego e de localização é regulada pelo artigo 9.º da Lei nº 32/2008, de 17 de Julho.

Por seu turno, os meios de obtenção de prova contemplados na Lei do Cibercrime, aplicam-se, com as devidas excepções, aos crimes previstos na mesma, aos crimes praticados através de sistema informático bem como em processos relativos a crimes em que seja necessário proceder à recolha de prova electrónica.

Ao invés, Paulo Dá Mesquita defende, que o artigo 14.º, bem como as restantes medidas processuais, acabaram por implicar a revogação do artigo 9.º da Lei nº 32/2008, de 17 de Julho.

Isto porque, a Lei do Cibercrime contempla no artigo 2.º alínea c) um conceito de "dados de tráfego" distinto do consagrado na Lei nº 32/2008, de 17 de Julho.

No entanto, para o Autor subsiste «a importância da Lei n.º 32/2008, sobretudo, no estabelecimento dos deveres dos fornecedores de serviços de conservação e protecção desses dados, bem como das condições técnicas operativas e destruição desses dados."[39]

[37] Rita Castanheira Neves, "As Ingerências nas Comunicações Electrónicas em Processo Penal", Coimbra Editora, 2009, p. 278.
[38] Rita Castanheira Neves, op. cit. p. 237.
[39] Paulo Dá Mesquita, op. cit. p. 98. Para o Autor a Lei nº 32/2008, de 17 de Julho consagra um conjunto de normas específicas sobre a conservação de dados gerados ou tratados, recorrendo a uma terminologia diferente da consagrada pela Lei do Cibercrime, nomeadamente recorrendo a

No Acórdão do Tribunal da Relação de Relação de Coimbra, de 26 de Fevereiro de 2014, foi invocado que o regime previsto no artigo 11.º, "é perfeitamente entendível e justificável pois o que está em causa é a obtenção de prova intangível que só pode corporizar-se no processo com a intervenção especializada e indispensável dos próprios operadores dos sistemas"[40].

Mais, "se não fosse estabelecido um regime especial como aquele que está definido no mencionado diploma, a investigação dos crimes nele previstos estaria condenada ao fracasso e estes crimes seguramente ficariam impunes já que apenas quanto aos crimes de catálogo seria então possível a obtenção dos dados pretendido."[41]

No entanto, é necessário fazer referência ao Acórdão do Tribunal de Justiça da União Europeia, que, no passado dia 8 de Abril declarou inválida a Directiva nº 2006/24/CE (que foi transposta para a ordem jurídica portuguesa através da Lei nº 32/2008, de 17 de Julho).

Para o Tribunal, a referida Directiva viola um conjunto de normas e princípios comunitários, nomeadamente, o princípio da proporcionalidade e reserva da vida privada dos cidadãos.

Foi considerado que a imposição às operadores de comunicações de conservação de dados de tráfego e de localização dos seus clientes, seja pelo período que for, representa uma intromissão desproporcionada e injustificável na vida privada dos cidadãos (em prol do combate contra a criminalidade grave).

Pode ser alegado que, tendo a decisão sido proferida pelo Tribunal de Justiça da União Europeia em sede de reenvio prejudicial (esta questão foi suscitada no Tribunal Federal austríaco e no Tribunal Superior irlandês, tendo remetido a questão para o Tribunal de

---

"um conceito mais restrito", excluindo os dados de conteúdo. Mais, alerta que poderão subsistirem questões decorrentes "de sobreposições normativas, em termos de vias de acesso processual penal a dados de tráfego subsumíveis a normas dos dois diplomas."

[40] Acórdão do Tribunal da Relação de Coimbra, de 26 de Fevereiro de 2014 – Proc. nº 559/12.0GBOBR-A.C1, consultável em: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/0e255b331c5eaecd80257c91005ae8bf?OpenDocument

[41] Acórdão do Tribunal da Relação de Coimbra, de 26 de Fevereiro de 2014 – Proc. nº 559/12.0GBOBR-A.C1, consultável em: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/0e255b331c5eaecd80257c91005ae8bf?OpenDocument.

Justiça da União Europeia), apenas vincula as partes que suscitaram a questão, não sendo tal decisão dotada de força obrigatória geral.

No entanto, tendo a Lei nº 32/2008, de 17 de Julho transposto para a ordem jurídica portuguesa a referida Directiva, a validade da mesma pode ser posta em causa, invocando-se a eventual violação do Direito da União Europeia.

Como alerta Pedro Venâncio, "relativamente às medidas previstas nos artigos 12.º a 15.º da Lei do Cibercrime, assume especial pertinência o disposto na Lei n.º 32/2008, de 17 de Julho."[42]

Tendo a presente Dissertação como objecto confrontar as disposições processuais previstas na Lei do Cibercrime com as disposições processuais previstas no Código de Processo Penal, a respeito da recolha de prova digital e procurar encontrar soluções legais de articulação entre as mesmas, e embora se trate de uma decisão jurisprudencial que poderá vir a ter implicações em alguns dos mecanismos processuais previstos na Lei do Cibercrime, fica apenas uma nota informativa a este respeito.

5.2 Análise das disposições processuais previstas no Capítulo III

Delimitado o âmbito de aplicação material das disposições processuais, cumpre neste momento, analisar cada meio de obtenção de prova previsto na Lei do Cibercrime.

Para Pedro Venâncio, "a consagração de disposições processuais relativas à preservação, revelação, apresentação, pesquisa e apreensão de dados informáticos (previstas nos artigos 12.º a 17.º da LC *)* impunha-se não só como um imperativo de direito internacional, face à ratificação da Convenção sobre Cibercrime, mas, acima de tudo, como uma inevitabilidade civilizacional."[43]

Assim, a Lei do Cibercrime prevê um conjunto de mecanismos processuais relativos à obtenção da prova digital, de carácter geral:

1. Preservação expedita de dados (artigo 12.º);
2. Revelação expedita de dados (artigo 13.º);

[42] Pedro Venâncio, As Disposições Processuais Relativas a Dados Informáticos na Lei do Cibercrime, JusJornal, N.º 1183, 24 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer.
[43] Pedro Venâncio, op. cit.

3. Injunção para apresentação ou acesso a dados (artigo 14.º);
4. Pesquisa informática (artigo 15.º);
5. Apreensão de dados informáticos (artigo 16.º);
6. Apreensão de correio elecrónico e registos de comunicações de natureza semelhante (artigo 17.º);

E, meios de obtenção de prova digital restritos a um conjunto determinado de crimes:

7. Intercepção de comunicações (artigo 18.º).;
8. Acções encobertas (artigo 19.º).

Os artigos 12.º ("preservação expedita de dados"), 13.º (revelação expedita de dados") e 14.º ("injunção para apresentação ou concessão do acesso a dados") preveem medidas processuais, de natureza cautelar.

Estamos perante diligências processuais que se encontram "relacionadas com elementos das comunicações electrónicas"[44] (e não com o acto comunicacional em si).

A Lei do Cibercrime prevê a possibilidade do Ministério Público e até dos órgãos de polícia criminal ordenarem a preservação expedita de dados, revelação expedita de dados e apresentação ou concessão de acesso a dados informáticos a determinadas entidades e cidadãos.

E podem exigir a preservação e a concessão de acesso a dados informáticos não só a "entidades públicas ou privadas, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático ou outra entidade que trate ou armazene dados informáticos" (noção de "fornecedor de serviço", previsto no artigo 2.º alínea d)), como a qualquer pessoa que tenha "disponibilidade ou controlo desses dados", conforme disposto no artigo 12.º número 1 e 4 bem como no artigo 14.º número 1.

O artigo 15.º ("pesquisa informática") tem correspondência com o artigo 19.º da Convenção sobre o Cibercrime e contempla o regime das pesquisas informáticas.

[44] Rita Castanheira Neves, op. cit. p. 277.

Estamos perante uma medida que, embora se denomine de "pesquisa" (o legislador optou por uma terminologia diversa da prevista na Convenção), acaba por consistir nas tradicionais buscas, adaptada, porém, ao ambiente digital.

O artigo 15.º número 6 sustenta tal afirmação ao remeter expressamente para a aplicação das regras e formalidades do regime das buscas, previsto no Código de Processo Penal.

A autoridade judiciária é a autoridade competente para autorizar ou ordenar, por despacho, a realização da referida diligência, tendo, sempre que possível, que presidir à mesma.

A título excepcional e nos casos previstos no artigo 15.º, número 3, podem os órgãos de polícia criminal proceder à pesquisa de dados informáticos sem a prévia autorização da autoridade judiciária.

No entanto, tal diligência deverá, nos termos do artigo 15.º número 4, ser imediatamente comunicada à autoridade judiciária competente, para que esta proceda à respectiva validação.

Deverá, igualmente, ser elaborado o relatório previsto no artigo 253.º do Código de Processo Penal e remetido à autoridade judiciária competente.

Paulo Dá Mesquita, refere que, embora "bem intencionados, no regime destas medidas ressaltam algumas das consequências negativas de uma construção normativa extravagante e desligada do código".[45]

Para o Autor, embora o legislador tenha adoptado uma terminologia diversa da estabelecida na Convenção, "continuam a valer os cânones estabelecidos no artigo 174.º número 1 do Código de Processo Penal."[46]

O artigo 16.º ("apreensão de dados informáticos") prevê o regime da apreensão de dados informáticos.

[45] Paulo Dá Mesquita, op. cit. p. 114.

[46] Paulo Dá Mesquita, op. cit. p. 115, ou seja:

1. "Quando houver indícios de que dados informáticos relacionados com um crime ou que possam servir de prova se encontram num determinado sistema informático é ordenada a busca informática:
2. A busca informática é ordenada por despacho pela autoridade judiciária competente, devendo esta, sempre que possível, presidir à diligência."

Tal como o regime da pesquisa de dados informáticos tem semelhanças com o regime das tradicionais buscas, também o regime da apreensão de dados informáticos acaba por ser uma adaptação (à realidade digital) das tradicionais apreensões, reguladas pelos artigos 177.º e seguintes do Código de Processo Penal.

À apreensão de dados informáticos aplicam-se as mesmas regras processuais que se aplicam à pesquisa de dados informáticos.

Assim, é a autoridade judiciária que tem competência pra autorizar ou ordenar a realização da apreensão, podendo esta apreensão ser levada a cabo sem a prévia autorização da autoridade judiciária quando se verifique "urgência ou perigo na demora", nos termos dos artigos 16.º número 1 e número 2.

Assim sendo, adaptando o regime das apreensões previstas no Código de Processo Penal à realidade digital, deve ter-se presente que são apreendidos os dados ou documentos informáticos de um determinado sistema informático que serviram ou foram destinados a servir a prática de um crime, bem assim como todos aqueles que tiverem sido deixados pelo agente no local do crime ou quaisquer outros susceptíveis de servir a prova.

Nos termos do artigo 16.º número 3, quando esteja em causa a apreensão de "dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular", os mesmos têm que ser apresentados ao juiz, só podendo ser juntos aos autos após uma ponderação, que deverá ter em conta "os interesses do caso concreto".

Esta norma acaba por "dar expressão normativa ao Acórdão nº 607/2003, do Tribunal Constitucional"[47][48].

Nos termos do artigo 16.º número 7, a apreensão de dados informáticos pode revestir várias modalidades.

Estamos perante uma disposição processual que, embora reflita o cuidado e o rigor que o legislador procurou demonstrar na construção sistemática da figura, acaba por ser "infeliz" ao abarcar no conceito de "apreensão" um conjunto de realidades distintas,

[47] Paulo Dá Mesquita, op. cit. p. 116.
[48] Acórdão nº 607/2003, do Tribunal Constitucional – Processo nº 594/03, publicado no Diário da República. (disponível em http://www.dre.pt/pdf2sdip/2004/04/084000000/0562405646.pdf).

acaba por misturar diversos conceitos ("apreensão", "cópia", "eliminação", "preservação").

Esta solução foi criticada por Paulo Dá Mesquita que considera que a redação da lei portuguesa foi "infeliz" uma vez que para "além de não ter suporte no código também contraria a terminologia da Convenção."[49]

A definição mais correcta de "apreensão" é aquela que se encontra prevista no artigo 16.º número 7 alínea a), sendo inclusive a definição que tem correspondência com artigo 178.º número 2, do Código de Processo Penal.

Quanto ao estabelecimento do âmbito de tutela do correio electrónico, o legislador adoptou um duplo tratamento: enquanto correspondência, por um lado e enquanto intromissão em comunicações electrónicas, por outro lado, "atendendo às especificidades dessa forma de comunicação."[50]

O artigo 17.º regula a "apreensão de correio electrónico e registos de comunicações de natureza semelhante."

Embora se encontre previsto um regime na Lei do Cibercrime para a apreensão de dados informáticos, o legislador foi mais além, e criou um regime específico para a apreensão de "correio electrónico e registos de comunicações de natureza semelhante."

E o carácter inovador deste meio de obtenção de prova, reside no facto não encontrar correspondência na Convenção sobre o Cibercrime.

Para Paulo Dá Mesquita, o conceito de "correio electrónico" "é amplo, abrangendo tanto os sistemas que utilizam o conglomerado de redes electrónicas de escala mundial (…) como sistemas de redes de computadores privados."[51]

No artigo 17.º remete-se expressamente para a aplicação do regime da apreensão de correspondência, regulado nos artigos 179.º e 252.º do Código de Processo Penal.[52]

[49] Paulo Dá Mesquita, op. cit. p.116. No entanto, o Autor considera que "apesar da infeliz redacção", o preceito prevê "na al. a) a forma de execução da apreensão de sistemas e dados informáticos (cf. art. 178.º º2, do CPP), n al. b) a cópia (e a respectiva execução) como alternativa à apreensão, e nas als. c) e d) do mesmo preceito como outras medidas possíveis a preservação de sistemas e dados informáticos, o bloqueio do acesso e a eliminação de dados informáticos."

[50] Paulo Dá Mesquita, op. cit. p. 118.

[51] Paulo Dá Mesquita, op. cit. p. 121.

Paulo Dá Mesquita alerta que a "tutela do artigo 179.º número 1 (e do 34.º da Constituição da República Portuguesa) reporta-se à comunicação em curso e não ao conteúdo de comunicação já acedida por parte do destinatário (que decide guardá-la)."[53]

Pedro Verdelho segue igualmente esta linha de pensamento, defendendo que o regime do artigo 17.º apenas se aplica quando esteja em causa a apreensão de comunicações de correio electrónico ou registos de natureza semelhante ainda não recebidas/lidas e armazenadas.

Se estivermos perante comunicações já recebidas/lidas e armazenadas, as mesmas deverão ser objecto de tratamento semelhante relativamente à apreensão de arquivo físico já recebido/lido e armazenado, podendo as autoridades criminais recorrer aos restantes mecanismos processuais previstos na Lei do Cibercrime, nomeadamente, o artigo 16.º (que regula a apreensão de dados informáticos)

Por seu turno, Rita Castanheira Neves segue uma posição diversa. Para a Autora, a ingerência nas mensagens de correio electrónico ou registos de natureza semelhante não deverá ser objecto de um triplo tratamento – como defende Paulo Dá Mesquita e Pedro Verdelho – mas sim de um duplo tratamento: enquanto intercepção nas comunicações, em tempo real e, enquanto comunicações armazenadas em suporte digital.

E socorre-se do argumento literal previsto no artigo 17.º Para a Autora, a expressão "armazenada" pressupõe que a comunicação já foi recebida/lida e, consequentemente, armazenada.

E, embora defenda que o artigo 17.º regula a apreensão das mensagens de correio electrónico e registos de natureza semelhante, reconhece que foi criado um desequilíbrio entre a ingerência nas comunicações armazenadas em suporte digital e a ingerência nos arquivos físicos, beneficiando as primeiras de uma tutela acrescida.

O artigo 18.º regula a "intercepção de comunicações" electrónicas e abarca as medidas processuais contempladas nos artigos 20.º e 21.º da Convenção sobre o Cibercrime.

[52] A análise deste artigo será levada a cabo no ponto seguinte.
[53] Paulo Dá Mesquita, op. cit. pp. 118 e seguintes.

Alerta-se que, até 2009, a intercepção de comunicações electrónicas seguia o regime processual das "escutas telefónicas", por remissão expressa do artigo 189.º número 1 do Código de Processo Penal.[54]

A Lei do Cibercrime, mais precisamente o artigo 18.º veio adaptar o regime das "escutas telefónicas" ao ambiente digital.

Para efeito da Lei do Cibercrime e, nos termos do artigo 2.º da Lei do Cibercrime, alínea e) é considerado intercepção "o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros."

Nos termos do artigo 18.º número 1, os órgãos de polícia criminal podem recorrer à intercepção de comunicações electrónicas em processos relativos a crimes:

i) "previstos na respectiva lei e
ii) cometidos por meio de um sistema informático ou, em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal."

Desta forma, a intercepção de comunicaões electrónicas acaba por ser outra forma de acesso legítimo a um determinado sistema informático, para além da pesquisa informática, regulada no artigo 15.º.

Quanto ao âmbito de aplicação material da diligência prevista no artigo 18.º, a doutrina não reúne consenso.

A maioria da doutrina considera que a intercepção de comunicações electrónicas pode ser utilizada em processos relativos a crimes:

1. Previstos na Lei do Cibercrime;
2. Praticados através de sistema informático e,
3. Em relação aos quais seja necessário proceder à recolha de prova electrónica, desde que os crimes se encontrem previstos no artigo 187.º número 1 do Código de Processo Penal

[54] Questão que vai ser abordada no próximo ponto.

Por seu turno, Paulo Pinto de Albuquerque considera que a norma do artigo 18.º número 1 deve ser interpretada no sentido de só ser admissível o recurso à interceção de comunicações em processos relativos a crimes "puníveis com pena de prisão superior, no seu máximo, a 3 anos."[55]

Nos termos do artigo 18.º número 3, a intercepção pode ter como objecto tanto "a recolha e registo de dados de tráfego (definidos no artigo 2.º, alínea c))" ou pode destinar-se "ao registo de dados relativos ao conteúdo das comunicações."

Ainda que se tenha procedido a uma autonomização do regime da intercepção de comunicações electrónicas para fora do Código de Processo Penal, nos termos do artigo 18.º número 4, devem aplicar-se, em tudo o que não contrariar o regime estatuído no artigo 18.º, as regras e formalidades previstas nos artigos 187.º e seguintes do Código de Processo Penal.

À semelhança do que sucede no ordenamento jurídico português – antes e depois da entrada em vigor da Lei do Cibecrime – no ordenamento jurídico alemão, o recurso à intercepção e gravação das comunicações, só é admissível em processos relativos a um conjunto específico de crimes.

A respectiva intercepção tem que ser autorizado ou ordenado por um juiz, embora em caso de "perigo na demora", o Ministério Público pode ordenar as mesmas. No entanto, terá que ser posteriormente validada por uma autoridade judicial.

Conforme disposto no número 2 da disposição legal citada, o despacho que ordene ou autorize a intercepção tem que conter qual o número de telefone ou "qualquer outra identificação da conexão estabelecida pela comunicação."[56]

Para Rita Castanheira Neves, esta norma é indicadora de que a intercepção e gravação de comunicações não se cinge apenas às comunicações telefónicas, permitindo-se a intromissão em comunicações de outra natureza.

Por seu turno, no ordenamento jurídico italiano, o legislador estipulou regimes processuais distintos em relação à intercepção e registo de comunicações: por um lado,

[55] Paulo Pinto de Albuquerque, "Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem", Editora Universidade Católica, 2011, Anotação 23, p. 549.
[56] Rita Castanheira Neves, op. cit. p. 105.

estipulou um regime específico para as comunicações orais e, por outro lado, um regime específico para as comunicações por via "informática ou telemática, ou seja, que pressupõe forma escrita, gráfica ou sonora."[57]

Quando ao artigo 19.º, que tem como epígrafe "acções encobertas", o mesmo determina a admissibilidade de "recurso às acções encobertas previstas na Lei nº 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:

i) " os previstos na presente lei;
ii) e os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos."

Estamos perante uma medida processual inovadora, na medida em que, tal como o artigo 17.º, não encontra correspondência na Convenção.

O artigo 19.º número 1, amplia a possibilidade de recurso à acção encoberta, prevendo um conjunto de crimes que não se encontram previstos na Lei nº 101/2001, de 25 de Agosto, ou seja, no Regime Jurídicos sobre as Acções Encobertas.

Paulo Dá Mesquita critica vivamente esta disposição processual, considerando que "a solução adoptada apresenta-se incorrecta ao descaracterizar a tabela desse regime, procedendo a uma associação inopinada entre crimes informátios, crimes cometidos através de um sistema informático e acção encoberta." [58]

Mais, para este Autor a solução adoptada pelo legislador ultrapassa, do ponto de vista jurídico-constitucional, "a linha do admissível, ao prever uma medida de carácter muito

[57] Rita Castanheira Neves, op. cit. p. 113.
[58] Paulo Dá Mesquita, op. cit. pp. 125 e seguintes.

excepcional para um leque muito amplo de crimes, sem aprofundamento normativo dos princípios da proporcionalidade e da necessidade."[59]

Rita Castanheira Neves segue a mesma linha de pensamento, considerando que a "atitude legislativa de flexibilização de alguns princípios básicos na condução da investigação criminal" acabam por fazer com que "cada vez mais se arrisque que o Estado perca a sua superioridade ética relativamente ao criminoso."[60]

Os artigos 22.º, 24.º e 25.º contemplam um conjunto de medidas de obtenção de prova de cariz internacional, no âmbito da cooperação internacional.

[59] Paulo Dá Mesquita, op. cit. pp. 125 e seguintes.
[60] Rita Castanheira Neves, op. cit. p. 282.

VI
CONFRONTO ENTRE OS MEIOS DE OBTENÇÃO DE PROVA PREVISTOS NA LEI DO CIBERCRIME E O CÓDIGO DE PROCESSO PENAL

6.1 A autonomização do regime de obtenção de prova digital com a Lei nº 109/2009, de 15 de Setembro

Podemos afirmar que existem duas fontes normativas que regulam o modo de obtenção da prova digital: a Lei do Cibercrime e o Código de Processo Penal.

Já analisadas as disposições processuais previstas na Lei do Cibercrime, cumpre agora dedicar a nossa atenção ao Código de Processo Penal.

Nos termos do artigo 189.º número 1, "o disposto nos artigos 187.º e 188.º (normas que regulam a intercepção e gravação de comunicações telefónicas) é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes."

Deste modo, podemos distinguir duas realidades (distintas) que se encontram inseridas nesta norma legal: por um lado, a intercepção e registo de comunicações ou conversações realizadas (em tempo real) através de um meio técnico diferente do telefone; e, por outro lado, as comunicações ou conversações electrónicas, nomeadamente correio electrónico, que se encontrem armazenadas em suporte digital (sublinhado nosso).

Ora, em 2009 entrou em vigor a Lei do Cibercrime, introduzindo um conjunto de mecanismos processuais destinados a regular e proporcionar a possibilidade de recolha de prova em ambiente digital.

Assim, e como afirma Paulo Dá Mesquita, "o correio eletrónico e as comunicações de natureza semelhante transmitidas através de sistemas informáticos passaram (desde 2009) a compreender, pelo menos, duas constelações com sedes normativas distintas: a

apreensão de correspondência do Código de Processo Penal e um regime específico de interceção e registo de comunicações de dados informáticos." [61]

Deste modo, surge a seguinte questão: qual será o âmbito de aplicação do artigo 189.º número 1 do Código de Processo Penal, com a entrada em vigor da Lei nº 109/2009, de 15 de Setembro?

6.2 Regime jurídico aplicável à ingerência nas comunicações armazenadas em suporte digital

O artigo 189.º número 1 do Código de Processo Penal determina a aplicação das regras e formalidades relativas ao regime da intercepção e gravação de comunicações telefónicas, quando esteja em causa a intromissão nas comunicações ou conversações já armazenadas em suporte digital.

Porém, a Lei do Cibercrime, veio contemplar uma solução legal diversa, estabelecendo um "novo e distinto regime jurídico[62]" para a ingerência nas comunicações armazenadas em suporte digital.

Assim, nos termos do artigo 17.º da Lei do Cibercrime, o "juiz poderá autorizar ou ordenar, por despacho, a apreensão" de comunicações electrónicas armazenadas em suporte digital, quando as mesmas "se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente, o regime da apreensão de correspondência previsto no Código de Processo Penal."

Mais, nos termos do artigo 11.º número 1, esta diligência por ser utilizada em processos relativos: aos crimes previstos na respectiva lei; aos crimes cometidos através de sistema informático e aos crimes em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

Assim, de acordo com o contemplado no Código de Processo Penal:

1. A intromissão nas comunicações já armazenadas em suporte digital deverá seguir o regime processual aplicável à intercepção e gravação de comunicações telefónicas (artigo 189.º número 1, segunda parte);

[61] Paulo Dá Mesquita, op. cit. p. 119.
[62] Rita Castanheira Neves, op. cit. p. 285.

2. Assim, só é permitido o recurso a este tipo de diligência em processos relativos aos crimes elencados no artigo 187.º número 1 (deixando de fora um conjunto significativo de crimes informáticos);
3. O recurso a este tipo de diligência só é permitido durante a fase do inquérito e "se houver razões para crer que a diligência é indispensável para a descoberta da verdade, ou que a prova seria, de outra forma, impossível ou muito difícil de obter."

Por seu turno, a Lei do Cibercrime estabelece:

1. A apreensão de correio electrónico ou registos de natureza semelhante pode ser levada a cabo em processos relativos aos crimes previstos na respectiva lei; aos crimes praticados através de sistema informático e aos crimes em que seja necessário proceder à recolha de prova em suporte electrónico (artigo 11.º número 1);
2. A referida diligência terá que se autorizada ou ordenada pelo juiz quando a referida apreensão seja "de grande interesse para a descoberta da verdade ou para a prova"; (artigo 17.º)
3. É aplicável "o regime de apreensão de correspondência previsto no Código de Processo Penal" (artigo 17.º).

Deste modo, os regimes processuais previstos na Lei do Cibercrime e no Código de Processo a respeito da ingerência nas comunicações electrónicas armazenadas em suporte digital são bastante distintos.

Notar que quando nos referimos a "comunicações electrónicas" pretendemos englobar as formas de transmissão de dados informáticos, via telemática, por meio distinto do "telefone."[63]

E, não tendo a Lei do Cibercrime procedido à revogação expressa do artigo 189.º número 1 do Código de Processo Penal, torna-se necessário analisar um conjunto de questões:

[63] No entanto, e como Paulo Dá Mesquita refere, estamos perante uma realidade bastante complexa, composta por um conjunto de elementos, que deveriam ter sido objecto de análise mais cuidada por parte do legislador.

1. A primeira consiste, desde logo, em saber qual o regime processual que deve ser aplicado quando esteja em causa a intromissão em comunicações electrónicas já armazenadas em suporte digital: deverá ser aplicado o regime consagrado no na da Lei do Cibercrime? Ou, por sua vez, o regime previsto no artigo 189.º número 1 do Código de Processo Penal, que remete para a aplicação do regime das "escutas telefónicas"?

2. A segunda questão passa por saber se, no caso de ser aplicado o regime estatuído no artigo 17.º - que remete para a aplicação das regras e formalidades consagradas nos artigos 179.º e 252.º do Código de Processo Penal - se referidas regras e formalidades aplicam-se na íntegra.

Paulo Dá Mesquita considera que o artigo 17.º da Lei do Cibercrime foi "o primeiro passo da directa revogação de algumas implicações do regime do Código de Processo Penal sobre intromissão em comunicações."[64]

Para este Autor, a extensão legal prevista no artigo 189.º número 1 do Código de Processo Penal deixa de se aplicar quando esteja em causa a apreensão de mensagens de correio electrónico e registos de comunicações de natureza semelhante.

O regime da apreensão de correio electrónico e registos de comunicações de natureza semelhante passa a ser regulado directamente pelo artigo 17.º da Lei do Cibercrime e, subsidiariamente (por remissão expressa do mesmo), pelos pressupostos e requisitos legais relativos à apreensão de correspondência, previstos nos artigos 179.º e 252.º (nº 2 e 3) do Código de Processo Penal.

Para este Autor, "apesar da redação pouco clara (do artigo 17.º), a remissão para as regras de processo penal sobre a apreensão de correspondência, parece implicar que a mesma reconduz o intérprete à teleologia do regime processual sobre a apreensão de correspondência."[65]

Também para Pedro Verdelho, ao regime da apreensão de correspondência eletrónica deve ser aplicado, por remissão expressa, o regime processual previsto nos artigos 179.º

[64] Paulo Dá Mesquita, op. cit. p. 117.

[65] Paulo Dá Mesquita, op. cit. p. 118.

e 252.º do Código de Processo Penal e não o artigo 187.º e seguintes (por remissão do artigo 189.º número 1).

Como refere, e bem, Rita Castanheira Neves, a previsão de um regime jurídico diverso do estatuído no Código de Processo Penal, permitiu ultrapassar a "intensa crítica que se fazia sentir à equiparação do correio electrónico armazenado em forma de suporte digital e ao correio em transmissão, para efeitos de remissão para o regime das escutas telefónicas."[66]

Isto porque, e seguindo a linha de pensamento da Autora, o carácter restritivo de admissibilidade desta diligência processual, "impedia o acesso a estes ficheiros em investigações relacionadas com crimes informáticos ou nas quais a prova só era possível de obter com recurso à prova digital." [67]

Agora, com o artigo 17.º, "passa a ser admitido o acesso e obtenção de correio electrónico em todas as investigações criminais cujo crime em causa esteja previsto na Lei nº 109/2009, seja cometido por meio de um sistema informático ou em relação ao qual seja necessário proceder à recolha de prova em suporte electrónico (nos termos do artigo11.º número 1)"[68].

Para Manuel Costa Andrade, o artigo 189.º número 1 do Código de Processo Penal contempla em si duas realidades distintas: por um lado, regula as comunicações/conversações, em tempo real, realizadas através de um meio técnico diferente do telefone e, por outro lado, regula as conversações/comunicações armazenadas em suporte digital, ou seja, o produto do acto comunicacional.

Tratando-se de duas realidades absolutamente distintas, as mesmas deveriam ser, por conseguinte, objecto de um tratamento legal distinto.

Para o Autor, o direito fundamental à inviolabilidade das telecomunicações, constitucionalmente consagrado no artigo 34.º (da Constituição da República Portuguesa), assegura "o livre desenvolvimento da personalidade de cada cidadão,

[66] Rita Castanheira Neves, op. cit. p. 274.
[67] Rita Castanheira Neves, op. cit. p. 274.
[68] Rita Castanheira Neves, op. cit. p. 274

nomeadamente através da troca, à distância de informações, notícias, pensamentos, opiniões, à margem da devassa da publicidade." [69]

O caso mais flagrante de restrição do direito fundamental da inviolabilidade das telecomunicações é o regime consagrado nos artigos 187.º e seguintes do Código de Processo Penal: a intercepção e gravação de comunicações ou "escutas telefónicas".

E, por se tratar de um instrumento processual extremamente intrusivo, o regime das "escutas telefónicas" tem um âmbito de aplicação bastante restrito, só podendo ser utilizado quando estejam em causa processos relativos ao elenco de crimes previstos no artigo 187.º número 1 do Código de Processo Penal.

Tal como foi referido no acórdão do Tribunal da Relação de Guimarães, de 29 de Março de 2011,[70] a redacção introduzida pelo legislador em 2007 ao artigo 189.º número 1, foi "infeliz" uma vez que incluíram no regime das "escutas telefónicas" o produto do acto comunicacional, que nada tem a ver com o fundo do regime, nomeadamente, a intromissão nas telecomunicações, tratando-se antes de meros arquivos digitais.

Antes da entrada em vigor da Lei do Cibercrime, e embora tivesse criticado a ampliação introduzida pela Reforma (do Código de Processo Penal) de 2007 ao artigo 189.º número 1, Manuel Costa Andrade considerava não ser defensável proceder a uma interpretação restritiva do mesmo uma vez que "com este sentido e alcance (isto é, no sentido de afastar a aplicação do regime das "escutas telefónicas" às comunicações electrónicas armazenadas em suporte digital), estaríamos perante uma redução teleológica "in malam partem", constitucionalmente insustentável."[71]

Ainda assim, até à entrada em vigor da Lei do Cibercrime, grande parte da jurisprudência fazia uma interpretação *contra legem* do artigo 189.º número 1 do Código de Processo Penal, considerando que as mensagens de correio electrónico ou

[69] Manuel Costa Andrade, *Bruscamente no verão passado*: a reforma do Código de Processo Penal –Observaões criticas sobre uma lei que podia e devia ter sido diferente, in RLJ, ano 137, nº 3950 e 3951, pp. 338.

[70] Acórdão consultável em: http://www.dgsi.pt/JTRG.NSF/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument.

[71] Manuel Costa Andrade op. cit. pp. 353/354.

registos de natureza semelhante armazenadas já lidas e armazenadas em suporte digital, deveriam ser objecto de tratamento legal semelhante ao "da carta em papel que, tendo sido recebida pelo correio e aberta, foi guardada em arquivo pessoal."[72]

O Acórdão da Relação de Lisboa de 15 de Julho de 2008 é exemplo dessa orientação.

O Tribunal considerou que, "na sua essência, a mensagem mantida em suporte digital depois de recebida e lida terá a mesma protecção da carta em papel que tenha sido recebida pelo correio e que foi aberta e guardada em arquivo pessoal."[73]

Ou seja, por que razão deveria a ingerência nas comunicações armazenadas em suporte digital ser objecto de uma tutela acrescida em relação aos arquivos físicos (recebidos ou não recebidos) quando nem sequer estamos perante um acto comunicacional mas sim perante o produto do acto comuncional ou seja, fora do âmbito das telecomunicações.

Não existe razão que justifique tal opção legislativa. Desconhecimento da dimensão e complexidade da realidade digital, talvez.

E a Lei do Cibercrime é reflexo desta linha de pensamento, ao ter consagrado regimes distintos para a intromissão nas comunicações em tempo real e nas comunicações armazenadas em suporte digital.

Para Pedro Venâncio, quando existam mensagens de correio electrónico que, embora não tenham sido interceptadas em tempo real mas que se encontrem armazenadas na "caixa do correio do destinatário, seja em servidor que preste serviço de armazenamento ou no próprio computador"[74] sejam relevantes para a descoberta da verdade, existem os "meios específicos previstos nos artigos 12.º a 17.º da Lei do Cibercrime", destinados a garantir o seu acesso.[75]

Deste modo, a doutrina - bem como a jurisprudência – reúne consenso quanto à desaplicação do artigo 189.º número 1 do Código de Processo Penal, relativamente na

[72] Ac. da Rel. de Guimarães de 12/10/2009, proc. n.º 1396/08.1PBGMR – A.G1). No mesmo sentido, o Ac.da Rel. do Porto, de 27/01/2010, proc. n.º 896/07.5JAPRT.P1; Acs. da Rel. de Coimbra, de 29/03/2006, proc. n.º 607/06; da Rel. de Lisboa de 20/03/2007, proc. n.º 7189/2006 – 7, e de 15/07/2008, proc. n.º 3453/2008 – 5.

[73] Acórdão da Relação de Lisboa de 15/07/08, Proc. nº 3453/2008.

[74] Pedro Venâncio, "A Intercepção de Comunicações e Acções Encobertas na Lei do Cibercrime" , JusJornal, N.º 1184, 25 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer.

[75] Pedo Vênancio, op. cit.

parte em que remete para o regime das "escutas telefónicas", a regulação da ingerência nas comunicações armazenadas em suporte digital.

6.3 Remissão do artigo 17.º para o regime da apreensão de correspondência previsto no Código de Processo Penal

Resolvida a primeira questão, cumpre agora determinar o âmbito da remissão feita pelo artigo 17.º para o regime da apreensão de correspondência previsto no Código de Processo Penal.

Para Pedro Verdelho, o regime de apreensão de correspondência previsto no Código de Processo Penal não é inteiramente aplicável ao regime estatuído no artigo 17.º da Lei do Cibercrime.

Nos termos do artigo 179.º do Código de Processo Penal:

1. A apreensão de correspondência só poderá ser ordenada ou autorizada quando existirem "fundadas razões para crer que: a) a correspondência foi expedida pelo suspeito ou lhes é dirigida, mesmo que sob nome diverso ou através de pessoa diversa; b) está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos e c) a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova" (artigo 179.º número 1);
2. A referida diligência terá ser previamente autorizada ou ordenada pela autoridade judicial, só sendo permitida, em casos excepcionais, que os órgãos de polícia criminal procedam à sua apreensão sem prévia autorização;
3. O juiz que tiver ordenado ou autorizado a apreensão "deverá ser o primeiro a tomar conhecimento do conteúdo da correspondência apreendida." (artigo 179.º número 3).

Pedro Verdelho defende a não aplicação do artigo 179.º número 1 do Código de Processo Penal, embora considere que "o artigo 17.º da Lei do Cibercrime não ignora os requisitos previstos no artigo (179.º número 1), tendo inclusive integrado um deles no regime do artigo 17.º (nomeadamente o requisito "quando a apreensão (…) se afigure ser de grande interesse para a descoberta da verdade ou para prova").[76]

[76] Pedro Verdelho, op. cit. p. 765.

Por conseguinte, "ao deixar de consagrar os restantes requisitos, fazendo a apreensão de correio elecrónico depender apenas deste (de a diligência "se afigurar ser de grande interesse para a descoberta da verdade ou para a prova", correspondente à alínea c) do número 1 do art. 179.º do Código de Processo Penal), (…) a lei pretendeu afastar a aplicação dos restantes." [77]

Rita Castanheira Neves considera que a remissão para o regime do Código de Processo Penal não abrange "a exigência de se tratar de crime punível com pena de prisão superior a três anos."[78]

Assim sendo, para a Autora, a remissão para o regime da apreensão de correspondência "parece, pois, realizada a quatro aspectos do regime"[79].

São eles:

1. A referência à nulidade, em caso de inobservância dos requisitos legais (artigo 179.º número 1 e 2);
2. Quando se tratar de correspondência electrónica que foi "expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa" (artigo 179.º, número 1, alínea a));
3. A apreensão de correspondência electrónica entre arguido e o seu defensor é proibida, "salvo se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime." (artigo 179.º número 2)
4. O juiz (que ordenou ou autorizou a diligência) deverá ser o primeiro a tomar conhecimento do conteúdo da correspondência electrónica apreendida (artigo 179.º número 3).

Quanto à intervenção judicial, Pedro Verdelho defende que o regime do artigo 17.º da Lei do Cibercrime tem que ser interpretado num sentido diverso do regime legal previsto nos artigos 179.º e 252.º do Código de Processo Penal.

De acordo com o Autor, "no caso de apreensão de correspondência eletrónica, a intervenção judicial (…) é sempre exigida em momento ulterior, portanto após se ter

[77] Pedro Verdelho, op. cit. p. 765.
[78] Rita Castanheira Neves, op. cit. p. 274.
[79] Rita Castanheira Neves, op. cit. p. 274.

encontrado este tipo de informação. Nessa altura, compete ao juiz escolher, de entre as mensagens encontradas as que são relevantes para a prova." [80]

É dado assente que as mensagens de correio electrónico (e os registos de comunicações de natureza semelhante) só podem ser juntas aos autos após intervenção judicial.

O que Pedro Verdelho defende é que essa intervenção judicial só pode acontecer após a apreensão – que neste caso será uma apreensão provisória – dado o objecto sobre que incide a referida diligência.

Assim, para Pedro Verdelho, o regime para a apreensão de correspondência previsto no Código de Processo Penal não deve ser totalmente aplicado ao regime previsto no art. 17.º da Lei do Cibercrime.

Rita Castanheira Neves considera que o juiz deve ser sempre o "primeiro a tomar conhecimento do conteúdo do correio electrónico e demais registos de comunicações apreendido, mandando-o juntar ao processo se o considerar relevante"[81].

No entanto, considera que se afigura "bastante prudente que se inverta tal lógica das coisas."[82]

Ou seja, para a Autora não se deixa de exigir que seja o juiz o primeiro a ter conhecimento do conteúdo das comunicações armazenadas em suporte digital. O que se deve exigir é que "para a eficácia da mesma (da diligência) devem seguir-se estritos critérios de abrangência, apenas apreendendo os e-mails que se afigurem realmente determinantes para a prova."[83]

6.4 Regime jurídico aplicável à intercepção e registo de comunicações electrónicas em tempo real

Até à entrada em vigor da Lei do Cibercrime, a intercepção e registo de comunicações electrónicas era regulada nos mesmos termos que a intercepção e gravação de comunicações telefónicas.

[80]Pedro Verdelho, *In:* Scientia Ivridica. - Braga : Universidade do Minho, 1951- . - T. 58, n.º 320 (2009), p. 764.

[81] Rita Castanheira Neves, op. cit. p. 275.
[82] Rita Castanheira Neves, op. cit. p. 275.
[83] Rita Castanheira Neves, op. cit. p. 275.

Assim, nos termos do Código de Processo Penal:

1. Só era permitido o uso desta diligência, em processos relativos aos crimes elencados no artigo 187.º número 1 (deixando de fora um conjunto significativo de crimes informáticos);
2. Só era permitida durante a fase do inquérito e se houvesse "razões para crer que a diligência é indispensável para a descoberta da verdade, ou que a prova seria, de outra forma, impossível ou muito difícil de obter."

A Lei do Cibercrime veio contemplar um regime específico para a intercepção e registo de comunicações electrónicas, através do artigo 18.º.

Tal como afirma Pedro Verdelho, o artigo 18.º acabou por legitimar o recurso ao regime da interceção de comunicações (electrónicas) em processos relativos a crimes, que até 2009 , não eram permitidos.

Assim, nos termos do artigo 18.º número 1 da Lei do Cibercrime, é possível recorrer à intercepção e registo de comunicações electrónicas em processos relativos:

1. Aos crimes previstos na respectiva lei;
2. Aos crimes praticados através de sistema informático ou,
3. Aos crimes em que seja necessário proceder à recolha de prova em suporte electrónico, desde que tais crimes se encontrem previstos no artigo 187.º número 1 do Código de Processo Penal.

Como já foi anteriormente mencionado[84], Paulo Pinto de Albuquerque considera que só é admitido o recurso a este tipo de diligência em processos relativos a crimes previstos na respectiva lei ou crimes praticados através de sistema informático, desde que tais crimes encontrem correspondência no artigo 187.º número 1 do Código de Processo Penal.

Não parece, porém, ser esse o entendimento da generalidade da doutrina.

Até porque o que se pretendeu com a Lei da Cibercrime, nomeadamente com a criação de um regime específico de recolha de prova digital, foi precisamente de corrigir o

[84] Ponto 5.2 da presente Dissertação, p. 24.

deficitário regime processual que vigorava no ordenamento jurídico português, em matéria de obtenção de prova digital.

Ao estar a limitar a possibilidade de recurso deste tipo de diligência - quando esteja em causa processos relativos a crimes praticados através de sistema informático - ao elenco dos crimes previstos no artigo 187.º número 1, acabam por não se verificar melhorias e soluções significativas que ajudem no trabalho das autoridades criminais contra este tipo de criminalidade.

Não obstante ter alargado o campo de aplicação, em comparação com o regime estatuído no artigo 187.º número 1 do Código de Processo Penal, o legislador acabou por transpor o regime da interceção de comunicações previsto no Código de Processo Penal para a Lei do Cibercrime.

Tal pode ser comprovado através do número 4 do artigo. 18.º, que determina que "em tudo o que não for contrariado pelo presente artigo, à interceção e registo de transmissões de dados informáticos é aplicável o regime da interceção e gravação de conversações ou comunicações telefónicas constantes dos artigos 187.º, 188.º e 190.º do Código de Processo Penal."

A verdade é que estamos perante a mesma diligência, ou seja, a intercepção de comunicações. No entanto, o objecto sobre que incide a diligência é distinto.

Os artigos 187.º e seguintes do Código de Processo Penal regulam a intercepção e gravação de comunicações telefónicas.

Por sua vez, o artigo 18.º regula a intercepção e registo de comunicações electrónicas.

Paulo Pinto de Albuquerque defende que o artigo 189.º número 1 do Código de Processo Penal não foi revogado pela Lei do Cibercrime, mantendo-se em vigor.

Pedro Verdelho segue a mesma orientação.

Mais, para o Autor, o artigo 189.º número 1 não deve ser revogado uma vez que não colide com o regime previsto no artigo 18.º da Lei do Cibercrime.

Segundo Pedro Verdelho, o artigo 18.º da Lei do Cibercrime veio instituir "um regime especial, destinado a ser aplicado em casos específicos, como resulta do respectivo artigo 11.º[85]

Paulo Dá Mesquita considera que o regime estatuído no artigo 18.º da Lei do Cibercrime "intersecta-se com dois problemas de articulação legal: os dispositivos sobre escutas telefónicas do Código de Processo Penal e a previsão do artigo 9.º da Lei nº 32/2008, de 17 de Julho sobre a transmissão de dados." [86]

Pelo facto da presente dissertação incidir somente sobre a articulação dos meios de obtenção de prova previstos na Lei do Cibercrime com o Código de Processo Penal, não se irá proceder à análise da Lei nº 32/2008, de 17 de Julho e as consequente disposição processual invocada.

Paulo Dá Mesquita, criticando "a recusa legislativa"[87] em estabelecer "um ponto de referência superador do artefacto telefone",[88] considera que estamos perante duas realidades distintas.

A interceção e registo de transmissão de comunicações electrónicas é uma realidade. Realidade distinta é a intercepção e gravação de conversações ou comunicações telefónicas.

No entanto, e como o Autor adverte que o termo "telefone" pode ser considerado como um "frágil referente distintivo"[89], pelo facto de também se verificar "digitalização das comunicações telefónicas"[90] que reconduz as mesmas "a comunicações transmitidas através de um sistema informático"[91].

Assim sendo, para o Autor, "o acesso, a interceção, o registo e a recolha de dados de conteúdo das telecomunicações eletrónicas"[92] encontra-se regulado na Lei do Cibercrime.

[85] Pedro Verdelho, op. cit. p. 746.
[86] Paulo Dá Mesquita, op. cit. p.119.
[87] Paulo Dá Mesquita, op. cit. p. 119.
[88] Paulo Dá Mesquita, op. cit. p. 119.
[89] Paulo Dá Mesquita, op. cit. p. 119.
[90] Paulo Dá Mesquita, op. cit. p. 119.
[91] Paulo Dá Mesquita, op. cit. p. 119.
[92] Paulo Dá Mesquita, op. cit. p. 119.

Ou seja, não se aplica o regime previsto no artigo 18.º da Lei do Cibercrime quando esteja em causa a intercepção e gravação de conversações ou comunicações telefónicas.

Quanto à remissão feita no artigo 18.º número 4 da Lei do Cibercrime, conclui-se que somente são aplicáveis as normas processuais previstas no Código de Processo Penal que não contrariem a Lei do Cibercrime.

Neste sentido, Paulo Dá Mesquita defende a revogação do artigo 189.º número 1 do Código de Processo Penal, considerando que este artigo não deve ser aplicado quando esteja em causa a interceção de comunicações eletrónicas uma vez que estas, a partir de 2009, passaram a ser reguladas pelo artigo 18.º da Lei do Cibercrime.

O Autor socorre-se da redacção do artigo 18.º, mais concretamente do número 4, que remete para a aplicação do regime previsto nos artigos 187.º e seguintes desde que "não contrarie o disposto" na Lei do Cibercrime.

Rita Castanheira Neves defende que o artigo 189.º número mantém-se em vigor. No entanto a Autora considera que "sobra pouco campo de aplicação" para o mesmo uma vez que sempre que se tratar de recolha de prova informática, "ter-se-á que recorrer à Lei nº 109/2009."

CONCLUSÕES

Embora o combate contra a criminalidade informática seja uma preocupação constante do legislador português, a verdade é que o regime jurídico de obtenção da prova digital só veio a ser implementado em 2009.

O legislador português limitou-se, até à entrada em vigor da Lei do Cibercrime, a englobar a realidade digital num único regime processual – o regime da intercepção e gravação de comunicações telefónicas – descurando das especificidades e componentes desta realidade.

Embora se encontre justificação e fundamento constitucional para a aplicação das regras relativas às "escutas telefónicas" à intercepção e registo de comunicações realizadas por meio técnico diferente do telefone – na medida em que estamos no domínio das telecomunicações, distinguindo-se somente o objecto sobre que incide a diligência – a mesma razão não se verifica quando se trata de ingerência nas comunicações armazenadas em suporte digital.

E a Lei do Cibercrime reflecte esta linha de entendimento quando regula, de forma distinta – tendo introduzido regimes assentes em princípios e linhas orientadoras distintas - a intercepção e registo de comunicações electrónicas (comunicações electrónicas aqui entendidas como comunicações levadas a cabo através de um meio técnico diferente do telefone) e a intromissão nas comunicações armazenadas em suporte digital.

Desta maneira, a Lei nº 109/2009, de 15 de Setembro – a "Lei do Cibercrime" – veio superar uma lacuna que existia em matéria de prova digital no ordenamento jurídico português.

No entanto, não tendo procedido a uma revogação expressa da disposição processual prevista no Código de Processo Penal, a questão que se colocava era a de saber qual âmbito de aplicação do artigo 189.º número 1 do Código de Processo Penal, com a entrada em vigor da Lei nº 109/2009, de 15 de Setembro.

Estamos perante várias disposições processuais previstas em diferentes diplomas com um ponto em comum: o facto de ambas regularem a forma de obtenção da prova digital.

Se por um lado temos um regime cuja admissibilidade é bastante restrito – dado o carácter intrusivo da diligência (artigo 187.º do Código de Processo Penal) – temos, por outro lado, um diploma que regula, de forma precisa, detalhada e especialmente com um âmbito de aplicação mais vasto, as várias diligências que podem ser utilizadas para recolha da prova digital, atendendo à complexidade da mesma.

Como referiu, e bem, Paulo Dá Mesquita, o legislador - aquando da Reforma de 2007 – ignorou "a diferença estrutural entre, por um lado, a mediação e transmissão comunicacional através de redes electrónicas e, por outro lado, os suportes electrónicos como simples forma de registo e arquivo."[93]

Mais grave ainda, foi ter conferido a estes últimos, "uma protecção distinta dos escritos e imagens em suporte de papel (ainda que todos apresentem as mesmas características em termos de relações de confiança comunicacional)."[94]

Como se constatou ao longo da presente exposição, a Lei do Cibercrime procurou adaptar os tradicionais meios de obtenção de prova – previstos no Código de Processo Penal – à realidade digital (as buscas e pesquisas informáticas, as apreensões e apreensões de dados informáticos, entre outros).

Assim, a Lei do Cibercrime estabeleceu um regime para a intercepção e registo de comunicações electrónicas – em tempo real – bem como um regime especificamente direcionado para a apreensão de correio electrónico (e registos de natureza semelhante) – ou seja, para a apreensão do produto do acto comunicacional.

Quanto ao regime da intercepção de comunicações electrónicas – contemplado no artigo 18.º da Lei do Cibercrime – o mesmo não se desviou (muito) dos princípios e requisitos exigidos para a intercepção de comunicações telefónicas.

Não havia razão atendível que justificasse a adopção de um regime totalmente distinto uma vez que, no fundo, estamos perante o mesmo tipo e grau de intromissão – ingerência nas comunicações em tempo real e, por conseguinte, objecto da mesma tutela constitucional - sofrendo somente desvios no âmbito material de aplicação da referida diligência, devido à natureza do objecto da mesma (realidade digital).

[93] Paulo Dá Mesquita, op. cit. p. 90.
[94] Paulo Dá Mesquita, op. cit. p. 91.

Desta forma, embora não seja do entendimento geral da doutrina a revogação do artigo 189.º número 1 - em relação à remissão para a aplicação do regime da intercepção e gravação de comunicações telefónicas à intercepção e registo das comunicações realizadas por meio técnico diverso do telefone – a verdade é que o mesmo deixa de ter aplicação prática, passando o artigo 18.º a ser a norma processual de referência para as autoridades criminais, em matéria de recolha de prova digital.

Assim, estamos perante duas realidades distintas: por um lado, a intercepção e registo de dados informáticos e, por outro lado, a intercepção e gravação de comunicações telefónicas.

Por seu turno, quando esteja em causa ingerência em comunicações armazenadas em suporte digital – designadamente correio electrónico ou registo de natureza semelhante – o regime aplicável deverá ser o previsto na Lei do Cibercrime e não o contemplado no artigo 189.º número 1 do Código de Processo Penal. E neste ponto a doutrina e jurisprudência a mesma linha de entendimento.

Desta maneira, quando esteja em causa a ingerência em comunicações armazenadas em suporte digital ou o acesso a dados informáticos armazenados em suporte digital, o regime aplicável será o que se encontra previsto na Lei do Cibercrime – nomeadamente o contemplado nos artigos 12.º a 17.º , consoante os casos - e já não o regime estatuído no artigo 189.º número 1 do Código de Processo Penal.

Tal como afirma Paulo Dá Mesquita, apesar de o legislador de 2009 não ter alterado, de forma expressa, o disposto no artigo 189.º número 1 do Código de Processo Penal, acabou por fazê-lo "envergonhadamente."[95]

Em jeito de conclusão, podemos afirmar que, com a entrada em vigor da Lei nº 109/2009, de 15 de Setembro, restou pouco campo prático para a aplicação do artigo 189.º, número 1 do Código de Processo Penal.

Assim, deve considerar-se o artigo 189.º número 1 parcialmente revogado - em relação à ingerência nas comunicações armazenadas em suporte digital - por força da "regulação mais completa e exaustiva"[96] da Lei nº 109/2009, de 15 de Setembro.

[95] Paulo Dá Mesquita, op. cit. p. 104.
[96] Paulo Dá Mesquita, op. cit. p. 102.

A ingerência nas comunicações armazenadas em suporte digital, passou a ser regulada, a partir de 2009, pelas disposições processuais previstas na Lei do Cibercrime e já não pelo artigo 189.º número 1 do Código de Processo Penal.

ACÓRDÃOS[97] E PARECERES

1. **Acórdão do Tribunal da Relação do Porto, de 27 de Janeiro de 2010;**
2. **Acórdão do Tribunal da Relação de Coimbra, de 11 de Janeiro de 2011;**
3. **Acórdão do Tribunal da Relação de Guimarães, de 29 de Março de 2011;**
4. **Acórdão do Tribunal da Relação de Évora, de 5 de Junho de 2012;**
5. **Acórdão do Tribunal da Relação de Guimarães, de 15 de Outubro de 2012;**
6. **Acórdão do Tribunal da Relação de Lisboa, de 22 de Janeiro de 2013;**
7. **Acórdão do Tribunal da Relação do Porto, de 22 de Janeiro de 2013;**
8. **Acórdão do Tribunal da Relação do Porto, de 24 de Abril de 2013;**
9. **Acórdão do Tribunal da Relação de Coimbra, de 26 de Fevereiro 2014;**
10. **Parecer nº 45/2012, da Procuradoria-Geral da República, de 21 de Janeiro de 2003[98] ;**
11. **Parecer da Procuradoria-Geral da República, de 24 Maio de 2012[99].**

[97] Consultáveis em: www.dgsi.pt.

[98]Parecer consultável em: http://jusjornal.wolterskluwer.pt/Content/DocumentView.aspx?params=H4sIAAAAAAAEAO29B2AcSZYlJi9tynt_SvVK1-B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVmVdZhZAzO2dvPfee--999577733ujudTif33_8_XGZkAWz2zkrayZ4hgKrIHz9-fB8_In7ROq-v3-Tv2s--s25e5O0nezsP7v3ue-d7OzsPf2FzvayW14vP3tTr_Be22aT5bPd3fzDdo__fo__v_8Js2q6z8mk1_WwPvxeX-Zts8tnuL2yrNitf5c1nB7-wqmd5_eT6s51f2MyrqxfZZXGRtUW1fJLVAraYzT77zlc79Nzbvffw_sEvvMzrhhp89pPFRb5s8184Ly7mz-n_rbTPmqZoTqqSumnyrJ7OX2YX-WeEw3pBzcdZs3r3C7OyzetlBoSCb3-yyK-kRbl8Sx--ZgCKR_PVkto3Wel_Kl08WbctYTRpl_Ld_wOgPZqlNQEAAA==WKE

[99] Parecer nº11/2011, consultável em **JusJornal**, N.º 1481, 11 de Junho de 2012.

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. CANOTILHO, J. J. GOMES; MOREIRA, VITAL, *Constituição da República Anotada,* Vol. I, 4ª Edição Revista, 2007;

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

5. MIRANDA, JORGE; MEDEIROS, RUI, *Constituição Portuguesa Anotada,* Tomo I, Coimbra Editora, 2005;

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

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

8. RODRIGUES, BENJAMIM, *Das Escutas Telefónicas – À Obtenção da Prova [Em Ambiente] Digital,* TOMO II, Coimbra Editora, 2009;

9. VENÂNCIO, PEDRO, *Lei do Cibercrime Anotada e Comentada,* Coimbra, Coimbra Editora, 2011;

--- **"**A Intercepção de Comunicações e Acções Encobertas na Lei do Cibercrime", JusJornal, N.º 1184, 25 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer

10. VERDELHO, PEDRO, *"*A obtenção de prova no ambiente digital", *Revista do Ministério Público,* Ano 25.º, nº 99 Julho-Setembro 2004 pp. 117-136;

--- "Apreensão de Correio Electrónico em Processo Penal", *Revista do Ministério Público,* Ano 25.º, nº 100, Outubro-Dezembro, 2004, pp. 153-164;

--- "Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital", *Revista CEJ,* 1º Semestre 2008, nº 9 – Jornadas sobre a Revisão do Código de Processo Penal, pp. 145-171;

11. VERDELHO, PEDRO; BRAVO, ROGÉRIO; ROCHA, MANUEL LOPES, *Leis do Cibercrime, Col.* PAULA VEIGA, Vol. I., Centroatlantico.pt, Portugal 2003.

ÍNDICE