A RECOLHA DE PROVA EM SUPORTE ELECTRÓNICO — EM PARTICULAR, A APREENSÃO DE CORREIO ELECTRÓNICO

Sónia Fidalgo

Resumo: um dos meios de obtenção de prova previstos na Lei do Cibercrime é a apreensão de correio electrónico e registos de comunicações de natureza semelhante. Neste artigo pretendemos apontar alguns dos problemas decorrentes do regime previsto na Lei do Cibercrime, designadamente, os que resultam da remissão para as normas do Código de Processo Penal sobre apreensão de correspondência.

Palavras-chave: apreensão de dados informáticos; apreensão de correio electrónico; registo de comunicações de natureza semelhante; actos do juiz.

I. AS DISPOSIÇÕES PROCESSUAIS DA LEI DO CIBERCRIME — ÂMBITO DE APLICAÇÃO[1]

1. Até à entrada em vigor da Lei do Cibercrime — Lei n.º 109/2009, de 15 de Setembro — não existiam entre nós regras especiais relativas à recolha de prova em suporte electrónico. A investigação dos crimes relacionados com a informática fazia-se recorrendo às regras gerais do Código de Processo Penal[2]. A Lei do Cibercrime trouxe, porém, novidades nesta matéria. Esta lei "estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas

---

1 O texto que agora se publica corresponde à conferência apresentada nas *V Jornadas Açorianas de Direito* (Ponta Delgada), em que, longe de aspirarmos a um tratamento profundo do tema, apontámos apenas alguns dos problemas decorrentes do regime das apreensões previsto na Lei do Cibercrime. Nesta publicação mantivemos o nosso propósito inicial, acrescentando apenas, em notas de rodapé, as referências bibliográficas estritamente necessárias.

2 Sobre a noção de criminalidade informática, cf. Costa, José de Faria / Moniz, Helena, «Algumas reflexões sobre a criminalidade informática em Portugal», *Boletim da Faculdade de Direito*, 73 (1997), p. 297 e ss., Marques, Garcia / Martins, Lourenço, *Direito da Informática*, 2.ª ed., Coimbra: Almedina, 2006, p. 639 e ss., e Venâncio, Pedro Dias, *Lei do Cibercrime Anotada e Comentada*, Coimbra: Coimbra Editora, 2011, p. 16 e ss.

ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa" (artigo 1.º).

A Lei do Cibercrime procurou, assim, condensar num só diploma legislativo todas as normas respeitantes à criminalidade informática: normas de direito substantivo, normas de direito processual e normas relativas à cooperação judiciária internacional.

Esta lei revogou a Lei da Criminalidade Informática — Lei n.º 109/91, de 17 de Agosto — e, num capítulo relativo a "disposições penais materiais" (capítulo II), consagrou os crimes de falsidade informática (artigo 3.º), dano relativo a programa ou outros dados informáticos (artigo 4.º), sabotagem informática (artigo 5.º), acesso ilegítimo (artigo 6.º), intercepção ilegítima (artigo 7.º) e reprodução ilegítima de programa protegido (artigo 8.º).

No capítulo sobre "disposições processuais" (Capítulo III), a lei prevê um conjunto de *novos* meios de obtenção de prova.

No capítulo sobre cooperação internacional (Capítulo IV), a lei consagra um conjunto de normas que complementam as disposições da Lei da Cooperação Judiciária Internacional em Matéria Penal (Lei n.º 144/99, de 31 de Agosto, com sucessivas alterações).

2. O artigo 11.º da Lei do Cibercrime define o âmbito de aplicação das disposições processuais. Esta norma estabelece que as regras processuais previstas, com excepção do disposto no artigo 18.º (intercepção de comunicações) e no artigo 19.º (acções encobertas), se aplicam: (a) a processos relativos aos crimes previstos na própria lei (nos artigos 3.º a 8.º); (b) a processos relativos a crimes cometidos por meio de um sistema informático (por exemplo, uma burla informática — artigo 221.º do Código Penal); e ainda (c) a processos relativos a crimes em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

A Lei do Cibercrime compreende, assim, um regime geral sobre recolha de prova em suporte electrónico, aplicável a processo por qualquer crime[3]; não se trata de regras processuais específicas para o sector da cibercriminalidade ou que se estendam também apenas aos processos por crimes praticados por meio de sistemas informáticos. Não se compreende, por isso, por que razão estas regras não foram inseridas no Código de Processo Penal[4].

---

[3] Sobre a distinção entre prova electrónica e prova digital, cf. RAMALHO, David Silva, *Métodos Ocultos de Investigação em Ambiente Digital*, Coimbra: Almedina, 2017, p. 98 e ss.

[4] Refutando os argumentos apresentados na Exposição de Motivos da Proposta de Lei n.º 289/X/4.ª para o enquadramento sistemático adoptado pelo legislador e defendendo que estas normas processuais deveriam ter sido inseridas no Código de Processo Penal, cf. MESQUITA, Paulo Dá, «Prolegómenos sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português — o Código e a Lei do Cibercrime», *in*: *Processo Penal,*

Se o legislador tivesse optado pelo enquadramento sistemático destas disposições no próprio Código de Processo Penal, talvez se tivessem evitado dificuldades de harmonização com normas do próprio Código (*v.g.*, artigos 179.º e 189.º) e de outros diplomas extravagantes (*v.g.*, normas da Lei n.º 32/2008, de 17 de Julho)[5].

II. PESQUISA E APREENSÃO DE DADOS INFORMÁTICOS

1. A dimensão processual da Lei do Cibercrime — artigos 12.º e ss. — é a mais inovadora e uma das mais importantes desta lei[6]. Por um lado, foram introduzidas na ordem jurídica portuguesa figuras processuais novas. Foi o que aconteceu com a preservação expedita de dados informáticos (artigo 12.º); com a revelação expedita de dados de tráfego (artigo 13.º); e com a injunção para apresentação ou concessão do acesso a dados informáticos (artigo 14.º). Por outro lado, foram adaptados ao ambiente informático ou digital institutos de processo penal já existentes no nosso ordenamento jurídico, adequando-os à realidade do ciberespaço. Foi o que se verificou com a pesquisa de dados informáticos (artigo 15.º), que corresponde à tradicional busca; a apreensão de dados informáticos (artigo 16.º); a apreensão de correio electrónico e registos de comunicações de natureza semelhante (artigo 17.º); e a intercepção de comunicações (artigo 18.º)[7]. Previu-se ainda um alargamento do âmbito de admissibilidade do recurso a acções encobertas (artigo 19.º).

Naturalmente, mantém-se a utilidade de certos meios de prova e de obtenção de prova previstos no Código de Processo Penal — designadamente, da prova pericial (artigo 151.º) e dos exames (artigos 171.º-173.º) — mesmo perante as especificidades que os sistemas informáticos suscitam[8]. Poderá ser necessário, por exemplo, que um perito informático transforme dados recolhidos num sistema informático em documentos legíveis.

2. No artigo 15.º da Lei do Cibercrime está regulada a pesquisa de dados informáticos armazenados num determinado sistema informático — expressão

---

Prova e Sistema Judiciário, Coimbra: Coimbra Editora, 2010, p. 98 e ss.; cf., ainda, Correia, João Conde, «Prova digital: as leis que temos e a lei que devíamos ter», *Revista do Ministério Público*, 139 (2014), p. 35.

5 Sobre estas dificuldades de harmonização, cf. Pinho, Carlos, «Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações»), *Revista do Ministério Público*, 129 (2012), p. 63 e ss.

6 Neste sentido também, Verdelho, Pedro, «A nova Lei do Cibercrime», *Scientia Iuridica*, LVIII (2009), p. 718 e p. 734, e 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: Coimbra Editora, 2011, p. 269.

7 Cf. Verdelho, Pedro, «A nova Lei do Cibercrime»…, cit., p. 734-735.

8 Cf. Verdelho, Pedro, «A nova Lei do Cibercrime»…, cit., p. 740, Venâncio, Pedro Dias, *Lei do Cibercrime*…, cit., p. 91-92, Correia, João Conde, «Prova digital…», cit., p. 50, e Ramalho, David Silva, *Métodos Ocultos de Investigação*…, cit., p. 134 e ss.

que a lei adoptou para aquilo que poderia designar-se *busca informática*. Por regra, é a autoridade judiciária competente — juiz ou Ministério Público — que autoriza ou ordena a realização da pesquisa, devendo, sempre que possível, presidir à diligência (artigo 15.º, n.º 1). Quanto à execução das pesquisas (artigo 15.º, n.º 6), são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal (artigos 174.º e ss.) e no Estatuto do Jornalista[9].

3. A Lei do Cibercrime prevê também a possibilidade de apreensão de dados informáticos. Nos termos do artigo 16.º, n.º 1, "quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos".

O legislador português mostrou preocupação com a protecção dos dados pessoais dos cidadãos, estabelecendo expressamente que "caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto" (artigo 16.º, n.º 3). Sempre que na fase de inquérito foram apreendidos, por exemplo, filmes, fotografias ou gravações sonoras que possam pôr em causa a privacidade dos sujeitos, o juiz de instrução deverá proceder a uma ponderação de interesses no caso concreto: por um lado, o interesse na salvaguarda da privacidade, por outro lado, os interesses que a investigação criminal visa prosseguir[10].

A apreensão de dados informáticos pode assumir diversas formas, tendo em conta os interesses do caso concreto e os princípios da adequação e da proporcionalidade (artigo 16.º, n.º 7). A apreensão de dados informáticos poderá fazer-se, designadamente, mediante: a) apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; b) realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; c) preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou d) elimi-

---

9 O Estatuto do Jornalista — Lei n.º 1/99, de 13 de Janeiro de 1999, alterada pela Lei n.º 64/2007, de 6 de Novembro, com rectificações feitas pela Declaração de Rectificação n.º 114/2007, de 13 de Dezembro de 2007 — estabelece expressamente que "a busca em órgãos de comunicação social só pode ser ordenada ou autorizada pelo juiz, o qual preside pessoalmente à diligência, avisando previamente o presidente da organização sindical dos jornalistas com maior representatividade para que o mesmo, ou um seu delegado, possa estar presente, sob reserva de confidencialidade" (artigo 11.º, n.º 6).

10 Cf. Verdelho, Pedro, «A nova Lei do Cibercrime»…, cit., p. 741-742.

nação não reversível ou bloqueio do acesso aos dados. Em rigor, apenas os dois primeiros procedimentos são verdadeiras formas de apreensão. Os últimos dois consubstanciam meios de protecção da prova ou de disposição dos dados informáticos no sistema inicial[11]. Apesar da referência expressa aos princípios da adequação e da proporcionalidade, na prática, razões de economia de tempo ditam que, por regra, os computadores portáteis sejam aprendidos, sendo posteriormente devolvidos ao seu titular.

III. APREENSÃO DE CORREIO ELECTRÓNICO E REGISTOS DE COMUNICAÇÕES DE NATUREZA SEMELHANTE

1. A Lei do Cibercrime estabelece um regime especial no caso de apreensão de correio electrónico e registos de comunicações de natureza semelhante, dispondo que "quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal" (artigo 17.º)[12].

O regime previsto neste artigo 17.º da Lei do Cibercrime tem gerado dificuldades de compatibilização com o disposto no Código de Processo Penal e tem dado lugar a interpretações doutrinais e jurisprudenciais diversas, sobretudo quando a apreensão se faz na fase de inquérito.

2. Nos termos do artigo 179.º, n.º 1, do Código de Processo Penal (apreensão de correspondência), o juiz só pode autorizar ou ordenar a apreensão de correspondência — é o *juiz* que autoriza ou ordena a diligência — quando estiver em causa um crime punível com pena de prisão superior, no seu máximo, a 3 anos (alínea *b)*). Nos termos do n.º 3 da mesma norma, o juiz que tiver autorizado ou ordenado a apreensão *é a primeira pessoa a*

---

11 Cf., nestes termos, Ramalho, David Silva, *Métodos Ocultos de Investigação*…, cit., p. 140, e Cardoso, Rui, «Apreensão de correio electrónico e registos de comunicações de natureza semelhante — artigo 17.º da Lei n.º 109/2009, de 15.IX», *Revista do Ministério Público*, 153 (2018), p. 173.

12 A Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, não tem disposições de natureza processual e a Convenção sobre o Cibercrime, que tem disposições desta natureza, não se refere expressamente à apreensão de correio electrónico, não tendo qualquer previsão específica semelhante à do artigo 17.º da Lei do Cibercrime. A origem desta norma está apenas na Proposta de Lei n.º 289/X/4.ª (artigo 19.º), que pretendeu adaptar o regime das buscas e apreensões previsto no Código de Processo Penal ao "ambiente do ciberespaço" (cf. Cardoso, Rui, «Apreensão de correio electrónico…», cit., p. 169-170).

tomar conhecimento do conteúdo da correspondência apreendida. Se o juiz considerar que a correspondência apreendida é relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a ao seu titular, não podendo ela ser usada como meio de prova. O juiz fica vinculado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova.

Nos termos do artigo 17.º da Lei do Cibercrime, à apreensão de correio electrónico e registos de comunicações de natureza semelhante aplica-se "correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal". Deverão as referidas normas do artigo 179.º do Código de Processo Penal aplicar-se também no caso de apreensão de correio electrónico?

2.1. Quanto ao pressuposto relativo ao crime em causa — crime punível com pena de prisão superior, no seu máximo, a 3 anos –, o problema que se coloca radica, desde logo, no facto de alguns dos tipos legais de crimes previstos na Lei do Cibercrime não serem puníveis com penas de prisão superiores a 3 anos[13].

Vimos já que o artigo 11.º da Lei do Cibercrime, ao delimitar o âmbito de aplicação das disposições processuais, estabelece que, com excepção do disposto no artigo 18.º (intercepção de comunicações) e no artigo 19.º (acções encobertas), tais disposições se aplicam a processos relativos aos crimes previstos na própria lei, a processos relativos a crimes cometidos por meio de um sistema informático e ainda a processos relativos a crimes em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

Nas normas relativas à intercepção de comunicações e à admissibilidade de recurso a acções encobertas, o legislador refere expressamente que tais meios processuais podem ser utilizados em processos relativos a crimes previstos na Lei do Cibercrime (artigos 18.º, n.º 1, alínea *a)*, e 19.º, n.º 1, alínea *a)*) e noutros processos por crimes que integrem o catálogo de crimes referido em cada uma das normas (artigos 18.º, n.º 1, alínea *b)*, e 19.º, n.º 1, alínea *b)*).

A conclusão a que se chega será a de que foi opção do legislador permitir a apreensão de correio electrónico e registos de comunicações de natureza semelhante sem a limitação decorrente de o crime ser punível com pena de prisão superior a 3 anos[14]. Permite-se, desta forma, a utilização deste meio de obtenção de prova em processos relativos aos crimes previstos na própria Lei do Cibercrime (como, aliás, acontece também com a intercepção de comunicações e as acções encobertas).

---

13 Veja-se as molduras penais previstas para os crimes de dano relativo a programas ou outros dados informáticos (artigo 4.º, n.ºs 1 e 3), acesso ilegítimo a sistema informático (artigo 6.º, n.ºs 1, 2 e 3), intercepção ilegítima de dados informáticos (artigo 7.º, n.ºs 1 e 3) e reprodução ilegítima de programa protegido (artigo 8.º, n.ºs 1 e 2).

14 Neste sentido, também, Neves, Rita Castanheira, *As ingerências nas comunicações electrónicas*…, cit., p. 274 e p. 276.

Temos dúvidas, no entanto, quanto à questão de saber se a intenção do legislador era a de que, afinal, a apreensão de correio electrónico possa ser usada em qualquer processo, por qualquer crime, em relação ao qual seja necessário proceder à recolha de prova em suporte electrónico — na prática, em qualquer processo penal, independentemente da gravidade do crime investigado.

2.2. Outra questão que se tem colocado está relacionada com a exigência de despacho judicial prévio, que autorize ou ordene a apreensão de mensagens de correio electrónico.

As respostas têm sido diversas. Há quem defenda que a apreensão só pode ser feita na sequência de um despacho judicial[15]. E há também quem entenda que a lei não é expressa a este propósito e que permite que se proceda a uma *apreensão cautelar* ou *provisória* de mensagens de correio electrónico mesmo que não tenha havido um despacho judicial anterior[16]. Esta apreensão será provisória porque as mensagens só serão efectivamente apreendidas e juntas ao processo se o juiz assim determinar. Se o juiz não autorizar a apreensão, então "a apreensão não se mantém, devendo o suporte das mensagens em causa ser devolvido ou, se a apreensão tiver sido feita por cópia, destruído"[17]. Esta interpretação da lei vai ao encontro de exigências práticas. De facto, por regra, as mensagens de correio electrónico são apreendidas no decurso de pesquisas informáticas, que têm lugar no âmbito de buscas. Pedro Verdelho salienta que, em regra, antes de uma busca ainda não se sabe se vai encontrar-se um computador; não se sabe se em tal computador vai encontrar-se mensagens de correio electrónico; e não poderá prever-se se tais mensagens vão ter interesse para a investigação. Deverá, então, entender-se, segundo o autor, que a lei permite que se faça uma *apreensão provisória* de mensagens de correio electrónico, no âmbito de pesquisas informáticas realizadas, por exemplo, com autorização do Ministério Público, sendo depois tais mensagens presentes ao juiz, para que este ordene a respectiva apreensão e junção ao processo[18].

Não nos parece, porém, que a lei não seja expressa a este propósito. Para além da remissão para o regime da apreensão de correspondência previsto no Código de Processo Penal (artigo 179.º, n.º 1), o próprio artigo 17.º da Lei do Cibercrime estabelece que *quando forem encontrados mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou*

---

15 Neste sentido, Neves, Rita Castanheira, *As ingerências nas comunicações electrónicas*..., cit., p. 275.

16 Verdelho, Pedro, «A nova Lei do Cibercrime»..., cit., p. 743.

17 Verdelho, Pedro, «A nova Lei do Cibercrime»..., cit., p. 743.

18 Verdelho, Pedro, «A nova Lei do Cibercrime»..., cit., p. 743-744. No mesmo sentido, cf. Cardoso, Rui, «Apreensão de correio electrónico...», cit., p. 179 e p. 195 e ss.

para a prova. A lei exige claramente um despacho judicial prévio a qualquer apreensão. Poderá questionar-se as dificuldades que tal exigência levanta na prática, mas não poderá dizer-se que a lei não faz esta exigência. Esta tem sido, também, a posição da nossa jurisprudência[19].

2.3. Outra questão que se tem colocado é a de saber se o juiz deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio electrónico apreendidas.

Há quem entenda que, ao contrário do que sucede com o correio físico, a lei não exige que o juiz seja o primeiro a tomar conhecimento do conteúdo das mensagens apreendidas — quem procede à pesquisa poderá encaminhar para o juiz mensagens concretas que aquele depois apreenderá ou não[20]. Entender-se que o juiz de instrução deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio electrónico ou semelhantes apreendidas põe em causa a própria *coerência do sistema de tutela de direitos*, na medida em que nos casos de intercepção de comunicações (artigo 18.º da Lei do Cibercrime) — potencialmente mais lesiva de direitos fundamentais — se permite que os órgãos de polícia criminal e o Ministério Público sejam os primeiros a tomar conhecimento do conteúdo das comunicações (artigos 18.º, n.º 4, da Lei do Cibercrime, e 188.º, n.ºs 1 a 4, do Código de Processo Penal)[21]. Já se afirmou, inclusivamente, que a exigência de que, no inquérito, seja o juiz de instrução o primeiro a conhecer o conteúdo das mensagens de correio electrónico apreendidas e a seleccionar aquelas que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova viola a estrutura acusatória do processo penal[22]/[23].

2.4. A nossa jurisprudência não tem sido, porém, sensível a estes argumentos. Entendendo que está em causa o direito à privacidade e ao sigilo da correspondência electrónica (artigos 26.º, n.º 1, e 34.º, n.º 4, da Constituição da República Portuguesa)[24], considera que a remissão que no artigo 17.º da

---

19 Veja-se, designadamente, o Acórdão do Tribunal da Relação de Guimarães de 29-03-2011 (Processo n.º 735/10.0GAPTL-A.G1) e os Acórdãos do Tribunal da Relação de Lisboa de 11-01-2011 (Processo n.º 5412/08.9TDLSB-A.L1-5), de 29-12-2017 (Processo n.º 184/12.5TELSB-A.L1) e de 06-02-2018 (Processo n.º 1950/17.0T9LSB-A.L1-5).

20 Precisamente nestes termos, Verdelho, Pedro, «A nova Lei do Cibercrime»…, cit., p. 744.

21 Neste sentido, Cardoso, Rui, «Apreensão de correio electrónico…», cit., p. 197 e ss.

22 Neste sentido, Cardoso, Rui, «Apreensão de correio electrónico…», cit., p. 204 e ss., esp.te p. 209.

23 Além destas razões de carácter material, invoca-se ainda a dificuldade prática que esta exigência envolve: as mensagens de correio electrónico são, por regra, apreendidas em grandes quantidades, não disponho o juiz de instrução das ferramentas que facilitam a análise de grandes quantidades de dados (cf. Neves, Rita Castanheira, *As ingerências nas comunicações electrónicas*…, cit., p. 275, Cardoso, Rui, «Apreensão de correio electrónico…», cit., p. 204, nota 47, e Nunes, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Coimbra: Gestlegal, 2018, p. 143).

24 Cf., neste aspecto concreto, o Acórdão do Tribunal da Relação de Lisboa de 29-12-2017 (Processo n.º 184/12.5TELSB-A.L1). Defendendo que o que está em causa na apreensão de

Lei do Cibercrime se faz para o regime de apreensão de correspondência previsto no Código de Processo Penal abrange o disposto no n.º 3 do artigo 179.º. Os nossos tribunais têm entendido que o juiz que autoriza ou ordena a diligência deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio electrónico apreendidas[25].

2.5. Mesmo após a entrada em vigor da Lei do Cibercrime há quem defenda uma distinção de regime conforme se trate da apreensão de correio electrónico aberto e lido pelo seu destinatário ou de mensagens de correio electrónico ainda não lidas. O correio electrónico recebido e lido deverá ser excluído do regime do artigo 17.º. Sendo considerado um mero documento, a sua apreensão deverá ser feita nos termos do regime da apreensão de dados informáticos, sendo suficiente a intervenção do Ministério Público com possibilidade de controlo judicial posterior, sempre que o conteúdo dos documentos apreendidos for susceptível de revelar dados pessoais ou íntimos que possam pôr em causa a privacidade do respectivo titular ou de terceiro (artigo 16.º, n.ºs 1 e 3, da Lei do Cibercrime). O regime *especial* previsto no artigo 17.º da Lei do Cibercrime justificar-se-á apenas em relação a mensagens de correio electrónico ainda não lidas pelo seu destinatário[26].

Não nos parece que tenha sido esta, porém, a opção do legislador. Na verdade, é possível, hoje, com um simples *clique*, marcar como lida uma mensagem de correio electrónico não lida e vice-versa. O sujeito pode aceder ao correio electrónico através de vários dispositivos e nuns deles a mensagem surgir como lida e noutros como não lida, dependendo do tipo de sincronização existente entre os diversos dispositivos. A fronteira entre correio electrónico lido e não lido é, assim, difícil de estabelecer. O legislador, reconhecendo o anacronismo e a inadequação daquela distinção de regimes, optou por atribuir uma tutela acrescida à mensagem em formato digital, submetendo-a ao regime

---

correio electrónico é o direito à autodeterminação informacional (e não o direito à inviolabilidade das comunicações), Nunes, Duarte Rodrigues, *Os meios de obtenção de prova*…, cit, p. 147. A este propósito, cf., também, Ramos, Vânia Costa, «Âmbito e Extensão do Segredo das Telecomunicações. Acórdão do Segundo Senado do Tribunal Constitucional Federal Alemão, de 2 de Março de 2006», *Revista do Ministério Público*, 112 (2007), p. 144 e ss., e Cardoso, Rui, «Apreensão de correio electrónico…», cit., p. 175 e ss. *Vide*, ainda, o Acórdão do Tribunal Constitucional n.º 403/2015 (Processo n.º 773/15).

25 Cf., neste sentido, os Acórdãos do Tribunal da Relação de Lisboa de 11-01-2011 (Processo n.º 5412/08.9TDLSB-A.L1-5), de 29-12-2017 (Processo n.º 184/12.5TELSB-A.L1) e de 06-02-2018 (Processo n.º 1950/17.0T9LSB-A.L1-5). Para tentar contrariar a dificuldade prática decorrente do facto de o correio electrónico ser geralmente apreendido em grandes quantidades, deverá exigir-se que durante a diligência se tenha sempre em atenção que para que a mesma seja eficaz devem-se seguir-se "critérios estritos de abrangência" e apreender apenas as mensagens de correio electrónico que se afigurem "realmente determinantes para a prova" (Neves, Rita Castanheira, *As ingerências nas comunicações electrónicas*…, cit., p. 275).

26 Neste sentido, Correia, João Conde, «Prova digital…», cit., p. 41; cf., também, Mesquita, Paulo Dá, «Prolegómenos sobre prova electrónica…, cit., p. 118, e Nunes, Duarte Rodrigues, *Os meios de obtenção de prova*…, cit. p. 145-146.

do artigo 17.º, independentemente de ter ou não sido lida pelo seu destinatário[27]. Tem sido este, também, o entendimento da nossa jurisprudência[28].

IV. CONCLUSÃO

Como referimos, a jurisprudência tem vindo a considerar que a apreensão de correio electrónico ou de registos de comunicações de natureza semelhante está dependente de um despacho judicial prévio e que o juiz que ordenou ou autorizou a diligência deve ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens apreendidas. Os nossos tribunais têm entendido que o despacho do Ministério Público que ordena a apreensão é nulo (artigos 17.º da Lei do Cibercrime e 179.º, n.º 1, do Código de Processo Penal) e que a omissão da análise da correspondência apreendida pelo juiz de instrução criminal — sendo este um acto da competência exclusiva deste juiz (artigo 268.º, n.º 1, alínea *d)*, do Código de Processo Penal) — constituirá uma nulidade nos termos do artigo 120.º, n.º 2, alínea *d)*, do Código de Processo Penal, por se tratar de um acto legalmente obrigatório. Tudo o que conduzirá, a final, segundo a jurisprudência, a que a prova que resulta dessa apreensão seja prova proibida, não podendo ser valorada (artigos 18.º, 32.º, n.º 8, e 34.º, n.º 4, da Constituição da República Portuguesa, e 126.º, n.º 3, do Código de Processo Penal)[29].

Enquanto a lei se mantiver com a redacção actual, não deve o Ministério Público, na sua função de direcção do inquérito, obedecendo em todas as intervenções processuais a critérios de estrita objectividade (artigo 53.º do Código de Processo Penal), deixar de requerer autorização judicial para apreensão de correio electrónico; não deve o juiz de instrução criminal deixar de ser a primeira pessoa a tomar conhecimento do conteúdo das mensagens de correio electrónico apreendidas, sob pena de, a final, se perderem elementos de grande interesse para a descoberta da verdade.

---

27 Neste sentido, também, Ramalho, David Silva, *Métodos Ocultos de Investigação*…, cit., p. 278-279, e Cardoso, Rui, «Apreensão de correio electrónico…», cit., p. 177 e p. 187 e ss.

28 Cf., a este propósito, o Acórdão do Tribunal da Relação de Lisboa de 29-12-2017 (Processo n.º 184/12.5TELSB-A.L1).

29 Cf. os Acórdãos do Tribunal da Relação de Lisboa de 29-12-2017 (Processo n.º 184/12.5TELSB-A.L1) e de 06-02-2018 (Processo n.º 1950/17.0T9LSB-A.L1-5). Cf., ainda a este propósito, Albuquerque, Paulo Pinto, *Comentário do Código de Processo Penal — à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4.ª ed., Lisboa: Universidade Católica Editora, 2011, p. 509-510, Cabral, Santos, «Artigo 179.º (Apreensão de correspondência)», *in*: *Código de Processo Penal Comentado*, 2.ª ed., Coimbra: Almedina, 2016, p. 708, e Correia, João Conde, «Artigo 179.º (Apreensão de correspondência)», *in*: *Comentário Judiciário do Código de Processo Penal*, tomo II, Coimbra: Almedina, 2018, § 33 e § 36.