
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VI – SETEMBRO/OUTUBRO DE 2018

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW by CIJIC

NOTAS DO EDITOR:

No prólogo de mais esta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antecipo-me a aduzir dois actos, em breve, solenes, que não deverão passar em claro nas agendas de cada um.

O primeiro desses actos terá lugar no próximo 17 de Outubro na Universidade de Aveiro. Trata-se da Sétima edição da Iniciativa Portuguesa do Fórum da Governação da Internet.

Um sublinhado desde logo para o local do evento. É importante que a academia se sinta interligada com Portugal, no seu todo. Sair de Lisboa, do conforto centralizador da capital, é um pequeno mas mui nobre sinal de que há muito e bom trabalho a ser desenvolvido diariamente na plenitude dos mais de 98 mil quilómetros quadrados que compõem o nosso pequeno país.

No que à edição deste ano do Fórum da Governação da Internet diz respeito, trata-se de um evento organizado pela FCT (Fundação para a Ciência e a Tecnologia I.P), em parceria com a ANACOM (Autoridade Nacional de Comunicações), APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da Informação), API (Associação Portuguesa de Imprensa), Associação DNS.PT, Ciência Viva (Agência Nacional para a Cultura Científica e Tecnológica), CNCS (Centro Nacional de Cibersegurança), IAPMEI (Agência para a Competitividade e Inovação), ISOC-PT

(Capítulo Português da ISOC), Polo TICE.PT, Secretaria Geral da Presidência do Conselho de Ministros, e Sociedade Civil.

Serão objecto de discussão, temas como «Governação e políticas públicas da Internet nos contextos nacional e global»; «Inteligência Artificial e *Big data*»; «Segurança no Ciberespaço: O dilema entre a privacidade do indivíduo e a segurança do Estado»; «Governação, confiança, privacidade e desafios na era do IoT»; «*Fake news, fake views* -Sociedade da (Des)Informação».

As sessões e respectivos painéis apresentam temas e oradores de reconhecida qualidade, e, seguramente, será um 17 de Outubro de 2018 muito e bem preenchido em Aveiro[1].

O outro evento, como seria natural, até pelo investimento feito pelo país na realização deste por mais dez anos em Portugal, é a *Lisboa web summit* 2018.

O programa e agenda[2] da feira, que se realizará no Altice Arena entre 5 e 8 de Novembro, já foram dados a conhecer. O destaque recai na presença de oradores como o Secretário-Geral das Nações Unidas, Sr. António Guterres; o inventor do *www*, Sir Tim Berners-Lee; o CEO do eBay, Mr. Devin Wenig; a Comissária Europeia para a Concorrência, Mrs. Margrethe Vestager; entre outros.

Os temas são vastos. A agenda *idem*. Uma semana desta feira para explorar avidamente.

Em suma, sendo eventos contrastantes na apresentação, na forma e até na finalidade, seria pouco cordial não aproveitar a proximidade destes para esta nota de agenda.

Arrolado o introito, focando-nos apenas no essencial desta nova edição, seguramente que a entrada em vigor, em pleno, do RGPD - *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE*; bem como da Lei Geral de Protecção de Dados (LGPD) no Brasil, aprovada no plenário do

1 Informações sobre o programa do evento podem ser consultadas em: https://www.governacaointernet.pt/pdf/forum_programa_2018.pdf.
O evento é de entrada livre mas requer uma inscrição prévia. Mais informações em: https://www.governacaointernet.pt/2018.html
2 Mais informações em: https://websummit.com/schedule

Senado Federal pelo PLC 53/2018, a 10 de Julho; impuseram que o tema da protecção de dados pessoais fizesse, novamente, parte do cardápio da revista.

No plano nacional, a Proposta de Lei 120/XIII, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, continua em suave desenvolvimento[3], mais de dois anos após a publicação do Regulamento europeu, o RGPD.

Não obstante, procurando contrariar o *adagio* da Proposta de Lei 120/XIII, procuramos coligir doutrina e opinião que demonstrem um pouco do *vivace* de pessoas e organizações na adaptação às novas realidades supranacionais. Neste sentido, encontraremos *ways not to read* o RGPD; as principais dificuldades e dúvidas partilhadas por organizações e por pessoas singulares na adaptação à nova realidade jurídica europeia. *Curiosamente*, do outro lado do Atlântico, trazemos, ainda, o impacto da LGPD brasileira nos negócios e nas pessoas, neste novel quadro normativo de agregação temática. É, pela actualidade do tema, tempo, ainda, de reintegrar o conceito de desindexação, *in casu*, da desindexação de conteúdos ofensivos na net, recuperando críticas jurídicas ao relevante caso *Google Spain*.

Saltando da circunspecção dos dados pessoais e da privacidade para outro tema, serão apresentadas reflexões quanto à apreensão de correio eletrónico e registos de comunicação de natureza semelhante. O tema é fervilhante. Na actualidade, a vivência em sociedade cresce *digitalodependente*, convocando discussões doutrinárias profundas. Ainda não será desta que se pacificará, entre os intérpretes e aplicadores do direito, a distinção juridicamente relevante entre correio e correio eletrónico. Mas, as reflexões que aqui se publicam, valem a leitura e o crepitar de questões.

Colocada em perspectiva esta espécie de matrimónio, de conveniência, que o direito e a tecnologia assumiram, a problemática dos drones, inteligência artificial e robótica, também têm aqui palco no plano jurídico.

Direito e Tecnologia são meios essenciais ao desenvolvimento do homem, com implicações, dilacerantes, nas mais variadas formas em como revelamos o ser social que somos. A ética, juridicamente relevante, aliada à segurança - subjacente ao

3 Pode ser consultada a actividade relativa à Proposta de lei em: http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

conceito *Safe-by-design* (SbD) - estimulam dissecções imediatas desde o plano de concepção, no patamar R&D do desenvolvimento das mais diversas ferramentas, utensílios, *gadgets*, cada vez mais apetrechadas de inteligência artificial e robótica, que vão procurando satisfazer necessidades diversas do *mercado*, isto é, nossas.

Aproveitando a epígrafe, projecto uma questão, que gostava de ver discutida numa próxima edição da revista: será profícuo que ao invés da pirexia em torno da segurança - a qualquer custo - dos dispositivos, tentando antecipar toda a indeterminabilidade da vida humana – com todos os custos inerentes a esta tarefa de adivinhação – o foco poderia vir a incidir sobre a *responsabilidade pela segurança*? Assumindo-se a impossibilidade de segurança absoluta de toda e qualquer ferramenta, será que alvitraremos, no futuro, um modelo de responsabilidades partilhadas como solução?

A insolência típica das muitas questões não poderia terminar sem o regresso a uma ideia em processo de maturação: como conciliar diversas ordens, práticas e tradições jurídicas; actores, partes e contrapartes processuais; pessoas singulares, organizações e Estados, perante tal amálgama de situações quotidianas neste *pot-pourri* que a Internet é e do qual dependemos? Estaremos no vértice da necessidade de um Tribunal Internacional para a Internet? Mais umas penadas sobre a arquitetura de um desejável edifício de harmonização e resolução de pleitos jurídicos a nível mundial.

Resta-me, por fim, agradecer a todos pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um sentido reconhecimento a cada um dos autores: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 05 de Outubro de 2018

Nuno Teixeira Castro

CYBERLAW

by CIJIC

DOUTRINA

ALGUMAS REFLEXÕES EM MATÉRIA APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÃO DE NATUREZA SEMELHANTE

O Acórdão do Tribunal da Relação de Lisboa de 6 de fevereiro de 2018

DUARTE RODRIGUES NUNES [1]

1 Juiz de Direito. Doutor em Direito pela Faculdade de Direito da Universidade de Lisboa. Contacto: duarterodriguesnunes@hotmail.com.

RESUMO

O Tribunal da Relação de Lisboa, no seu Acórdão de 6 de fevereiro de 2018, considerou que o regime da apreensão de correspondência previsto no Código de Processo Penal é aplicável na sua totalidade à apreensão de correio eletrónico e comunicações de natureza semelhante. Os criminosos utilizam as vantagens proporcionadas pelas novas tecnologias para preparar ou executar crimes e suprimir as provas do seu cometimento, usufruindo da rapidez e da volatilidade das novas formas de comunicação à distância. O artigo 17.º da Lei n.º 109/2009, de 15 de setembro, equipara o correio eletrónico e as comunicações de natureza semelhante (SMS e MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via *Whatsapp, Viber, Skype, Facebook*, etc.) ao correio tradicional para efeitos de apreensão. Pelas enormes diferenças entre o correio eletrónico e o correio tradicional e pelas dificuldades que a aplicação do regime da apreensão de correspondência suscita, a apreensão de correio eletrónico e comunicações de natureza semelhante deveria ser regulada pelo regime geral da apreensão de dados informáticos. O regime da apreensão da correspondência previsto no Código de Processo Penal deverá ser aplicado *cum grano salis* e *mutatis mutandis* à apreensão de correio eletrónico e registos de comunicação de natureza semelhante.

Palavras-Chave: Cibercrime – Prova digital – Correio eletrónico – Apreensão – Direito à intimidade/privacidade.

ABSTRACT

In its Judgment of February 6th, 2018, the Lisbon Court of Appeal found that the seizure of correspondence provided for in the Code of Criminal Procedure is applicable in its entirety to the seizure of electronic mail and communications of a similar nature. Criminals use the advantages offered by new technologies to prepare or execute crimes and suppress evidence, taking advantage of the speed and volatility of new forms of distance communication. Article 17 of Law no. 109/2009, of September 15th, equates electronic mail and communications of a similar nature (SMS and MMS, conversations in *Messenger*, voice messages related to communications or sound files and/or picture via *Whatsapp, Viber, Skype, Facebook*, etc.) to traditional mail for the purpose of seizure. Due to the enormous differences between electronic mail and traditional mail and the difficulties that the application of the regime of seizure of correspondence gives rise to, the seizure of electronic mail and communications of a similar nature should be governed by the general regime for the seizure of computer data. The rules of seizure of correspondence provided for in the Code of Criminal Procedure should be applied *cum grano salis* and *mutatis mutandis* to the seizure of electronic mail and communication records of a similar nature.

Keywords:Cybercrime – Digital evidence – E-mail – Seizure – Privacy.

SUMÁRIO: 1. Introdução. 2. As circunstâncias do caso concreto. 3. A utilidade/necessidade da apreensão de correio eletrónico e registos de comunicação de natureza semelhante para a investigação criminal. 4. O regime da apreensão de correio eletrónico no Direito português. 5. A evolução da regulamentação da apreensão de correio eletrónico no Direito português. 6. Da (des)adequação da equiparação do correio eletrónico ao correio tradicional. 7. Todos os aspetos do regime da apreensão de correspondência deverão ser aplicados, e nos mesmos tempos, à apreensão de correio eletrónico e registos de comunicação de natureza semelhante? 8. Conclusões. Bibliografia. Jurisprudência.

1. INTRODUÇÃO

O Tribunal da Relação de Lisboa, no seu Acórdão de 6 de fevereiro de 2018 (Processo 1950/17.0 T9LSB-A.L1-5)[1], concedeu provimento ao recurso interposto pelo Ministério Público, revogando o despacho recorrido e determinando a sua substituição por outro que determine que o Juiz de Instrução Criminal seja a pessoa a tomar conhecimento em primeiro lugar do correio eletrónico apreendido, disponível, copiado pelo perito, em ficheiros legíveis.

Para tal, o Tribunal entendeu que, sujeitando o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, a apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante ao regime de apreensão de correspondência previsto no Código de Processo Penal, o n.º 3 o artigo 179.º desse Código estabelece que o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, o que, por conseguinte, se aplica ao correio eletrónico já convertido em ficheiro legível, constituindo ato da competência exclusiva do Juiz de Instrução Criminal, nos termos da al. d) do n.º 1 do artigo 268.º do Código de Processo Penal. A inobservância de tal formalidade constitui a sua violação nulidade expressa absoluta e que se reconduz, afinal, ao regime de proibição de prova; ademais, a falta de exame da correspondência pelo juiz constitui uma nulidade prevista na al. d) do n.º 2 do artigo 120.º do Código de Processo Penal, porque se trata de um ato processual legalmente obrigatório.

Mais afirma o Tribunal da Relação de Lisboa que, em caso de urgência, isto é de possível perda de informações úteis à investigação de um crime em caso de demora, o juiz pode

1 *In www.dgsi.pt.*

sempre autorizar a abertura imediata de correspondência (assim como de correio eletrónico) pelo órgão de política criminal, que também poderá ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, nos termos dos n.ºs 2 e 3 do artigo 252.º do Código de Processo Penal, devendo a ordem policial ser convalidada no prazo de 48 horas, sob pena de devolução ao destinatário caso não seja atempadamente convalidada, ou caso seja rejeitada a convalidação.

E, em conclusão, afirma-se no aresto sob análise que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, remete expressamente para o regime da apreensão de correspondência previsto no Código de Processo Penal, sem redução do seu âmbito, impondo-se, por isso, a aplicação de tal regime na sua totalidade.

O entendimento do Tribunal da Relação suscita, na nossa ótica, desde logo, as questões (1) da bondade da opção do legislador em submeter a apreensão de correio eletrónico já recebido ao regime da apreensão de correspondência e (2), independentemente de tal bondade, se a remissão que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, opera para o regime de apreensão de correspondência previsto no Código de Processo Penal inclui todo e qualquer aspeto deste regime.

2. AS CIRCUNSTÂNCIAS DO CASO CONCRETO

Com relevância para o presente artigo, as circunstâncias do caso concreto são as seguintes:

a) Por despacho proferido a 16 de março de 2017, o Ministério Público ordenou a realização de buscas não domiciliárias e concedeu autorização para pesquisa, em suportes informáticos, com vista à apreensão de documentação guardada em suporte digital e armazenada em sistema informático;
b) No dia 24 de março de 2017 foram realizadas as buscas ordenadas durante as quais foi efetuada apreensão de variado material informático, dentre ele, computadores, *tablets*, discos externos e efetuada pesquisa informática em equipamentos portáteis, discos e *pen's*;
c) Foi efetuada cópia desses ficheiros com a advertência explícita de que, caso fossem encontradas mensagens de correio eletrónico em tais suportes, as mesmas deveriam ser gravadas em suporte autónomo sem qualquer acesso ou

visualização do respetivo conteúdo, em consonância com o que havia sido judicialmente determinado nos mandados de buscas domiciliárias;

d) A 18 de agosto de 2017, foram copiadas mensagens de correio eletrónico, através de ficheiros encapsulados, para disco rígido autónomo, sem qualquer visionamento do respetivo conteúdo, selado para posterior apreciação judicial;

e) O Ministério Público, a 25 de outubro de 2017, determinou a apresentação de todos os elementos de correio eletrónico colocado em suporte autónomo e revelados pelos exames, para que o Juiz de Instrução Criminal deles tomasse conhecimento em primeiro lugar;

f) O Juiz de Instrução Criminal proferiu o seguinte despacho: «*Tendo sido os e-mails apreendidos na sequência de busca realizada por determinação do Ministério Público tal não significa, por razões de coerência sistemática, que os mesmos tenham de ser visualizados em primeiro lugar pelo Juiz de Instrução Criminal.*

Na verdade, caso os mesmos tivessem sido objecto de intercepção nos termos dos arts. 187.° n° 1 al. a) e 189.° do CPP, poderiam ter sido visualizados pelo OPC e pelo Ministério Público em primeiro lugar, sendo apresentados já após selecção ao Juiz de Instrução Criminal para ulterior validação em conformidade com o art. 188.° n°s 4 e 6 do CPP.

Assim, sendo não se vislumbra fundamento de ordem interpretativa ou sistemática para que os e-mails apreendidos nos termos do art. 17.° da Lei 109/2009 de 15.09 sejam objecto de tratamento diverso, mais garantístico do que o relativo à apreensão directa de telecomunicações, por aplicação estrita do regime do art. 179.° do CPP, remissão que deve ser entendida apenas garante do sigilo profissional, designadamente de Advogado.
Pelo exposto, deverá o OPC proceder à visualização dos e-mails e demais dados apreendidos, devendo apresentar relatório para validação após tal diligência, nos termos e para os efeitos do art. 188.° n°s 4 e 6 do CPP.»;

g) O Ministério Público interpôs recurso de tal despacho, esgrimindo, entre outros, os seguintes argumentos:

- O entendimento plasmado no despacho recorrido viola o disposto nos artigos 17.º da Lei 109/2009, de 15 de setembro, e 179.º, n.º 3 do Código de Processo Penal, normas que exigem que o juiz seja o primeiro a tomar conhecimento do

correio eletrónico copiado, a fim de expurgar dos autos todos os elementos cujo conhecimento esteja vedado aos demais sujeitos processuais;

- A remissão operada pelo artigo 17.º da Lei 109/2009, de 15 de setembro, não poderá significar outra coisa que não a aplicação dos procedimentos para a apreensão de correspondência para a obtenção de prova válida no que respeita ao correio eletrónico;

- O legislador processual separou na Lei do Cibercrime dois regimes distintos, cabendo um para as interceções de correio eletrónico, ao qual são aplicáveis as regras relativas a interceções telefónicas do Código de Processo Penal e o segundo, para as apreensões de correspondência eletrónica, ao qual, também por remissão, são aplicadas as normas de apreensão de correspondência do Código de Processo Penal, pelo que, crendo que o legislador se soube exprimir convenientemente, a cada regime pertencerá um procedimento diverso, não havendo como considerar que um é menos garantístico que o outro, sendo apenas diverso;

3. A UTILIDADE/NECESSIDADE DA APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÃO DE NATUREZA SEMELHANTE PARA A INVESTIGAÇÃO CRIMINAL

Como se afirma no Relatório Explicativo da Convenção sobre o Cibercrime[2], «*A revolução nas tecnologias da informação operou mudanças fundamentais na sociedade e irá provavelmente continuar a fazê-lo num futuro previsível. Foram inúmeras as tarefas cuja execução se tornou mais fácil. Enquanto, inicialmente, apenas alguns sectores específicos da sociedade procederam a uma racionalização dos seus métodos de trabalho, com a ajuda das tecnologias da informação, atualmente, não existe praticamente nenhum sector da sociedade que não tenha sido abrangido pelas mesmas. As tecnologias da informação vieram, de uma forma ou de outra, conferir novos contornos a quase todos os aspetos das atividades do Homem.*

2 *In https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf* (pesquisa em 06/06/2018).

Uma característica notável da tecnologia da informação reside no impacto que esta teve, e ainda virá a ter certamente, na evolução da tecnologia das telecomunicações. Os clássicos sistemas telefónicos, envolvendo a transmissão da voz do Homem, foram suplantados por sistemas de permuta de grandes quantidades de dados, incluindo sob a forma de voz, texto e música, assim como de imagens estáticas e móveis. Esta permuta não se dá apenas entre os seres humanos, mas também entre estes e os computadores, e ao nível dos sistemas de computadores entre si. As ligações por comutação de circuitos foram substituídas por ligações por comutação de pacotes. Nos dias de hoje, já não é importante o facto de se poder ou não estabelecer uma ligação direta; basta que os dados em questão sejam introduzidos numa rede com um endereço de destino ou que sejam disponibilizados a todos quantos desejem aceder-lhes.

A utilização universal do correio eletrónico e o acesso aos inúmeros sites através da Internet constituem o exemplo desses desenvolvimentos que tão profundamente contribuíram para a mudança ocorrida na nossa sociedade.

A fácil acessibilidade e pesquisa da informação contida em sistemas informáticos, aliada às possibilidades quase ilimitadas relativamente à sua permuta e difusão, não obstante as distâncias geográficas, traduziu-se por um crescimento explosivo da quantidade de informação disponível e do conhecimento que daí advém.

Estes desenvolvimentos deram origem a mutações sociais e económicas sem precedentes, mas apresentam simultaneamente uma faceta negativa: a emergência de novos tipos de criminalidade, bem como a prática dos crimes tradicionais com recurso às novas tecnologias. Além disso, as consequências do comportamento de índole criminosa poderão ser mais extensas e ter um maior alcance uma vez que não são restringidas por quaisquer limites geográficos ou fronteiras nacionais. A recente disseminação de vírus informáticos prejudiciais, um pouco por todo o mundo, comprova esta realidade. As medidas de carácter técnico que visam proteger os sistemas informáticos deverão, pois, ser tomadas concomitantemente com medidas de natureza jurídica a fim de evitar e deter a prática de crimes.».

De facto, as vantagens proporcionadas pelas novas tecnologias tanto podem ser aproveitadas para fins lícitos como para fins ilícitos, Com efeito, de acordo com o saber adquirido, o correio eletrónico e outros meios de comunicação similares (SMS e MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via *Whatsapp, Viber, Skype, Facebook*) são amplamente utilizados pelos

criminosos para preparar e executar crimes e para suprimir as provas do seu cometimento, usufruindo da rapidez, anonimato e volatilidade das comunicações informáticas, o que dificulta de sobremaneira a sua deteção e, quando sejam utilizadas medidas antiforenses como a encriptação das mensagens ou o recurso à *Dark Web*, a sua interceção e gravação. Ademais, o correio eletrónico e outros meios de comunicação similares, pela sua natureza de meios de comunicação à distância, permitem suplantar a distância (muitas vezes, na ordem de centenas ou milhares de quilómetros) entre os criminosos comparticipantes e/ou entre os criminosos e as vítimas, para comunicarem entre si ou para cometer crimes que, de outro modo, jamais conseguiriam cometer[3].

Assim, o correio eletrónico e outros meios de comunicação similares, ao permitirem enviar todo o tipo de anexos, poderão ser utilizados para difundir/instalar em sistemas informáticos alheios toda a espécie de *malware*[4], que, uma vez instalado nesses sistemas informáticos, permitirá obter credenciais de acesso (ao *home banking*, a cartões de débito ou crédito, ao *e-mail*, a redes sociais ou a *sites* de natureza reservada que requerem a introdução de uma *password*), copiar ou aceder a dados armazenados nesse sistema (por exemplo, para exercer chantagem sobre a vítima ou para espionagem industrial) ou vigiar toda a atividade aí desenvolvida[5]. E também para abordar as vítimas para, posteriormente, as burlar (como sucedeu com as famosas "Cartas da Nigéria" ou burlas 4-1-9[6]).

Do mesmo modo, no caso da criminalidade organizada transnacional (onde podemos incluir o terrorismo internacional e a grande criminalidade económica, que tende a ser levada a cabo em vários países, incluindo paraísos fiscais), estando os criminosos em países diversos terão de recorrer a meios de comunicação à distância para comunicarem entre si, mas não só.

---

3 *V.g.* burlas cometidas através da Internet ou *phishing*, em que, por exemplo, o criminoso poderá estar num dado país da Europa e as vítimas (muitas vezes, centenas ou milhares de pessoas) poderão estar em qualquer outra parte do Mundo.

De facto, utilizando sistemas informáticos e a Internet, os Cibercriminosos conseguem, fruto da possibilidade de envio de *e-mails* em massa, infetar milhares de sistemas informáticos em todo o Mundo num relativamente curto espaço de tempo. Do mesmo modo, os ataques do tipo DoS (*Denial of Service*) ou DDoS (*Distributed Denial of Service*), que consistem no envio massivo, em simultâneo, de pedidos para um dado sistema informático (ou vários sistemas, no caso do DDoS), só serão possíveis com a utilização de meios que permitam esse envio massivo simultâneo, de molde a que o sistema informático fique desativado por via desse envio massivo de pedidos, que "consome" o CPU e a memória.

4 O *malware* é um programa informático que visa permitir a quem o utiliza infiltrar-se num sistema informático alheio, com o intuito de causar prejuízos ou de obter informações (confidenciais ou não), que, de outro modo, não poderia obter. O *malware* pode aparecer sob a forma de código executável, scripts de conteúdo ativo, etc.

5 Cfr. ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, pp. 24, 35 e 59, e MISHA GLENNY, Darkmarket, p. 11.

6 Relativamente às "burlas 4-1-9-", *vide*, entre outros, ALBANESE, Organized Crime in Our Times, 5.ª Edição, pp. 224-225, e ABADINSKY, Organized crime, 9.ª Edição, p. 206.

Assim, no caso de organizações criminosas transnacionais que se expandem para outros países, muitas vezes utilizando a emigração de nacionais do seu país de origem, os membros da cúpula tendem a estar no país de origem, existindo depois "células" da organização noutros países. Mas também pode suceder que, por via de uma repressão eficaz no país de origem, a "cúpula" da organização tenha de se deslocar para um outro Estado em que a repressão seja menos eficaz ou não exista e tenha necessidade de comunicar com os membros que ficaram no país de origem. E também não podemos esquecer que as organizações criminosas, para se protegerem da atuação das autoridades, costumam manter reservada a identidade dos membros que ocupam as posições mais elevadas na hierarquia, mesmo relativamente aos demais membros ou aos colaboradores externos.

E, no caso das organizações terroristas, o recurso às novas tecnologias de comunicação tanto pode servir para a proteção da organização como para a prossecução da sua finalidade terrorista (*v.g.* para realizar ataques terroristas, propaganda, captação de futuros membros e simpatizantes da causa, comunicação entre o núcleo central as várias "células" independentes e coordenação entre os vários componentes da organização, obtenção de informações úteis para a organização, transferência de capitais, obtenção de lucro por via de burlas cometidas através da Internet, etc.), conferindo uma enorme rapidez e um anonimato absoluto ou quase absoluto às comunicações, potenciando a capacidade operacional da organização e dificultando enormemente a tarefa das entidades cuja missão é evitar os atentados terroristas, desmantelar organizações terroristas e perseguir e punir os seus membros e apoiantes.

Um dos domínios em que mais se lança mão dos meios informáticos para a proteção de criminosos face às autoridades é ao nível do branqueamento de capitais, ao ponto de se afirmar que a informática é um meio *essencial* para o branqueamento e que o branqueamento só se consolidou como atividade conatural da criminalidade organizada com a possibilidade recorrer às novas tecnologias e de se entender que existe uma relação de "conexão necessária" entre a criminalidade organizada, o branqueamento de capitais e a criminalidade informática[7].

Por isso, houve que adaptar as leis penais a estas novas realidades, de molde a permitir a sua regulação jurídica, desde logo mediante a criação de novos tipos de crime informático-digitais (designadamente os previstos nos artigos 4.º a 9.º da revogada Lei n.º 109/91, de 17 de agosto e, atualmente, nos artigos 3.º a 8.º da Lei n.º 109/2009, de 15 de setembro). E, para além

7 Cfr. GUTIÉRREZ FRANCÉS, "Las altas tecnologías de la información al servicio del blanqueo de capitales transnacional", *in* Blanqueo de Dinero y Corrupción en el Sistema Bancario, Delitos Financieros, Fraude y Corrupción en Europa, II, pp. 194-196 e 209.

da alteração das leis penais, houve que criar regras processuais penais, onde se incluem as relativas a meios de obtenção de prova específicos para a investigação destes tipos de crime. Com efeito, dificilmente meios de obtenção de prova criados para obter informações constantes de suportes corpóreos serão adequados para obter informações incorpóreas como aquelas que constam de dados informáticos[8].

Um dos meios de comunicação proporcionados pelas novas tecnologias da informação e comunicação é o correio eletrónico, que, seguindo o conceito legal constante da al. b) do n.º 1 do artigo 2.º da Lei n.º 41/2004, de 18 de agosto, na redação que lhe foi dada pela Lei n.º 46/2012, de 29 de agosto, definimos como «*qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha*». E, *ad latus* do correio eletrónico, encontramos outros veículos de comunicação como as SMS e MMS, conversações

8 Na aceção da al. b) do artigo 2.º da Lei n.º 109/2009, de 15 de setembro, onde se definem dados informáticos como «*qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função*».

Na verdade, como se afirma no Relatório Explicativo da Convenção sobre o Cibercrime, « *O presente Artigo visa a modernização e a harmonização das legislações nacionais relativamente à busca e apreensão de dados informatizados armazenados, para fins de obtenção de provas relacionadas com investigações criminais ou ações penais específicas. Qualquer legislação interna em matéria de direito processual penal, contempla os poderes relativos à busca e apreensão de objetos tangíveis. Contudo, em muitos Estados ou jurisdições, os dados informatizados armazenados, por si só, não serão considerados como algo tangível, pelo que não poderão ser adquiridos a título de investigações criminais e ações penais da mesma forma que os bens corpóreos, a não ser através da obtenção do suporte no qual se encontram armazenados os dados. O objetivo do Artigo 19º da presente Convenção é o de estabelecer um poder equivalente relativo aos dados armazenados. (…).*

Todavia, no que se refere à investigação de dados informatizados, são necessárias disposições processuais complementares, a fim de assegurar que os dados informatizados podem ser obtidos com a mesma eficácia de uma operação de busca e apreensão de suportes de dados tangíveis. Existem diversas razões para este facto: em primeiro lugar, os dados são intangíveis, como é o caso dos dados sob a forma eletromagnética. Em segundo lugar, enquanto que os dados podem lidos através da utilização de um equipamento informático, o mesmo não se passa relativamente à apreensão e transporte desses mesmos dados, tal como acontece com um documento em suporte papel. O suporte físico no qual se encontram armazenados os dados intangíveis (por exemplo, o disco rígido de um computador ou uma disquete) deverá ser apreendido e retirado do local, ou deverá ser efetuada uma cópia dos dados, quer sob uma forma tangível (por exemplo, uma impressão feita a partir de um computador) quer sob uma forma intangível, num suporte físico (por exemplo, uma disquete), antes que o suporte tangível que contém a cópia possa ser apreendido e transportado para fora do local. Nos dois últimos casos enunciados, em que são efetuadas cópias dos dados, permanecerá no sistema informático ou na unidade de armazenamento uma cópia dos dados. A legislação nacional deverá instituir o poder relativo à realização das ditas cópias. Em terceiro lugar, devido à conectividade dos sistemas informáticos, os dados poderão não se encontrar armazenados no computador alvo de busca, podendo ser facilmente acessíveis a partir desse mesmo sistema. Os dados poderão ser armazenados numa unidade de armazenamento de dados associada, que se encontre diretamente ligada ao computador, ou indiretamente ligada ao mesmo através do recurso a sistemas de comunicação, tais como a Internet. Tal poderá requerer ou não a implementação de novas leis no sentido de alargar a extensão da busca ao sistema no qual os dados se encontrem efetivamente armazenados (ou da extração dos dados do local em questão para o computador alvo de busca), ou de maneira a permitir a utilização dos tradicionais poderes de investigação, com uma maior rapidez e uma melhor coordenação, em ambos os locais.».

no *Messenger*, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via *Whatsapp, Viber, Skype, Facebook,* etc.

Ora, como referimos, no caso de criminosos que se encontrem em locais diversos[9] ou que, por qualquer razão, optem por comunicar entre si à distância em lugar de se encontrarem presencialmente, estes meios de comunicação, pela sua rapidez (permitindo suplantar milhares de quilómetros em apenas alguns segundos), volatilidade e dificuldade de deteção e interceção/gravação são mecanismos que irão ser certamente utilizados. E também poderá ser utilizado para infetar sistemas informáticos com *malware* para obter credenciais de acesso, copiar ou aceder a dados informáticos ou vigiar toda a atividade desenvolvida em sistemas informáticos alheios. Por isso mesmo, a obtenção do conteúdo dessas comunicações será tendencialmente decisivo para o êxito das investigações.

Ciente desta realidade, o legislador português regulou, na Lei n.º 109/2009, de 15 de setembro, diversos meios de obtenção de prova que permitam a tomada de conhecimento do conteúdo dessas comunicações, como sucede com os meios de obtenção de prova previstos nos artigos 17.º (apreensão de correio eletrónico e registos de comunicações de natureza semelhante) e 18.º (interceção de comunicações) dessa Lei. A diferença entre ambos os meios de obtenção de prova radica no facto de, enquanto, no caso da interceção de comunicações, a obtenção de tais informações ocorre no decurso do processo comunicacional, na apreensão de correio eletrónico e registos de comunicações de natureza semelhante[10], o processo comunicacional já terminou.

No presente artigo iremos apenas analisar a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, prevista no artigo 17.º da Lei n.º 109/2009, de 15 de setembro.

9 *V.g.* os membros de uma organização criminosa que se encontrem no país de origem dessa organização face aos membros de células dessa organização que se encontram em países estrangeiros, onde se instalaram aproveitando-se da emigração de nacionais do país onde a organização está sedeada.

10 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, p. 510, RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 274, PEDRO DIAS VENÂNCIO, Lei do Cibercrime, pp. 100 e 116, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, pp. 117 e ss., e Acórdãos da Relação de Lisboa de 11/01/2011 e 29/03/2012, da Relação do Porto de 07/07/2016, da Relação de Évora de 06/01/2015 e 20/01/2015 e da Relação de Guimarães de 29/03/2011, *in www.dgsi.pt*.

4. O REGIME DA APREENSÃO DE CORREIO ELETRÓNICO NO DIREITO PORTUGUÊS.

Nos termos do artigo 17.º da Lei n.º 109/2009, de 15 de setembro, «*Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.*»[11].

Assim, de acordo com o referido preceito, a apreensão de correio eletrónico e registos de comunicações de natureza semelhante (como SMS, MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações via *Whatsapp, Viber, Skype, Facebook, etc.*) que se encontrem armazenados no sistema informático que tenha sido acedido pelas autoridades terá de ser autorizada pelo Juiz, sempre que essa apreensão se mostre de grande interesse para a descoberta da verdade ou para a prova e esteja em causa a investigação de crimes previstos na Lei n.º 109/2009, de 15 de setembro, cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico[12], sendo aplicável o regime da apreensão da correspondência, previsto nos artigos 179.º e 252.º do Código de Processo Penal[13]. Porém, pela especificidade do correio eletrónico face ao correio tradicional, consideramos que a remissão que artigo 17.º da Lei n.º 109/2009, de 15 de setembro, opera para o regime da apreensão da correspondência previsto no Código de

11 Contudo, sempre que a pessoa que tenha recebido as mensagens de correio eletrónico ou os registos de comunicações de natureza semelhante preste consentimento para que as autoridades tomem conhecimento do teor das mesmas e sejam transcritas e juntas aos autos ou proceda ela própria à junção aos autos da mensagem em causa, não há que aplicar o regime do artigo 17.º da Lei n.º 109/2009, de 15 de setembro (cfr. Acórdãos da Relação de Lisboa de 29/03/2012 e da Relação do Porto de 22/05/2013, *in www.dgsi.pt*).

12 Ou seja, este meio de obtenção de prova poderá ser aplicado a um universo de crimes aberto (cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 147, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, p. 98, e Acórdãos da Relação de Évora de 06/01/2015 e 20/01/2015, *in www.dgsi.pt*).

13 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, p. 510, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, p. 118, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 765, e Acórdãos da Relação de Lisboa de 11/01/2011 e 06/02/2018, *in www.dgsi.pt*; contra, ARMANDO RAMOS, "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, pp. 56-57.

Processo Penal deverá ser lida *cum grano salis* e *mutatis mutandis*[14] e sem prejuízo de tal opção legislativa ser de bondade muito duvidosa.

5. A EVOLUÇÃO DA REGULAMENTAÇÃO DA APREENSÃO DE CORREIO ELETRÓNICO NO DIREITO PORTUGUÊS

A Lei n.º 109/2009, de 15 de setembro, regulou, pela primeira vez, no nosso ordenamento jurídico, meios de obtenção de prova em matéria de Cibercrime[15], apesar de a Convenção sobre o Cibercrime já datar de 23/11/2001 (tendo sido assinada por Portugal nessa mesma data) e ter entrado em vigor em 01/07/2004[16] e de ser inequívoca a insuficiência dos meios de obtenção de prova previstos no Código de Processo Penal (claramente pensados para a obtenção de provas "corpóreas") para investigar eficazmente a criminalidade informática, mas não só.

Antes da entrada em vigor da Lei n.º 109/2009, de 15 de setembro, e até à entrada em vigor das alterações introduzidas no Código de Processo Penal pela Lei n.º 48/2007, de 29 de agosto, na ausência de regulamentação em matéria de apreensão de correio eletrónico, a

14 No que tange ao regime jurídico da apreensão de correio eletrónico e registos de comunicações de natureza semelhante, com maiores desenvolvimentos, *vide* DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 139 e ss.

15 Em que, adotando um conceito amplo, incluímos os crimes que ofendem bens diretamente ligados ao meio informático (*v.g.* o acesso ilegítimo), que visam proteger o próprio uso da informática e os seus aspetos característicos como o *software* e a navegação na Internet, bem como os crimes que lesam bens jurídicos "tradicionais" (*v.g.* a honra ou o património), mas que são cometidos através do uso de sistemas informáticos (o que aumenta especialmente a perigosidade ou danosidade para os bens jurídicos lesados e dificulta a deteção do seu cometimento e da identidade do agente, justificando a especial atenção do Direito penal). De resto, fazendo cada vez menos sentido diferenciar o plano do Direito penal material do plano do Direito processual penal, a delimitação do conceito de Cibercrime deverá ter em conta, por um lado, a determinação das condutas criminosas que devam ser incluídas no âmbito da criminalidade informática e, por outro, a determinação das condutas criminosas relativamente às quais se mostre necessário lançar mão de meios investigatórios especificamente direcionados para a obtenção de prova digital.

E, se atentarmos na Lei n.º 109/2009, de 15 de setembro, verificamos que o legislador adotou um conceito amplo de Cibercrime, pois, por um lado, apenas incluiu nela condutas criminosas em que o elemento digital surge como parte integradora do tipo legal e como seu objeto de proteção, mas, na vertente processual penal, determinou, no n.º 1 do artigo 11.º, que, salvo no caso da interceção de comunicações eletrónicas (artigo 18.º) e das ações encobertas em ambiente informático-digital (artigo 19.º), os meios de obtenção de prova aí previstos aplicam-se a processos relativos a crimes previstos nessa lei e também a crimes cometidos por meio de um sistema informático e a crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

E o mesmo sucede com os autores da Convenção sobre o Cibercrime, atento o elenco legal de condutas cuja criminalização é imposta e o âmbito das disposições processuais penais e relativas à cooperação judiciária em matéria penal.

16 Sendo que a introdução na nossa ordem jurídica, de meios de obtenção de prova específicos para a investigação do Cibercrime não dependia, nem da entrada em vigor da Convenção nem da sua transposição para o Direito português.

Doutrina e a Jurisprudência defendiam a aplicação dos meios de obtenção de prova "tradicionais" (designadamente os previstos no Código de Processo Penal) na investigação do Cibercrime, sendo que, no que tange à apreensão de mensagens de correio eletrónico, defendia-se a equiparação, em termos de regime jurídico, do correio eletrónico ao correio tradicional[17].

Na medida em que, pela generalização do uso deste meio de comunicação à distância, a apreensão de correio eletrónico se revelava cada vez mais essencial para investigar a prática de crimes, era esta a única forma de, de acordo com a lei vigente, viabilizar a utilização deste meio de obtenção de prova.

Ciente da necessidade de regular a apreensão do correio eletrónico, o legislador, com a reforma de 2007 do Código de Processo Penal, regulou pela primeira vez a apreensão de correio eletrónico. Assim, no n.º 1 do artigo 189.º, determinou que a apreensão de correio eletrónico, ainda que armazenado em suporte digital[18], é regulada pelo regime das escutas telefónicas, operando, desse modo, uma equiparação do correio eletrónico às escutas telefónicas. No fundo, o legislador submeteu ao regime das escutas telefónicas, quer a interceção em tempo real quer a apreensão das mensagens de correio eletrónico, ou seja, submeteu ao regime de um meio de obtenção de prova cuja utilização implica uma intervenção num processo comunicacional alheio (as escutas telefónicas) uma situação em que ocorre uma tal intervenção (interceção em tempo real de mensagens de correio eletrónico) e outra em que tal não ocorre (apreensão das mensagens de correio eletrónico).

Todavia, apesar de ser louvável a intenção do legislador de regular a apreensão (e a interceção) de correio eletrónico, um tal regime só poderia ter-se por desajustado no que tange à apreensão de correio eletrónico já recebido pelo destinatário, por várias razões.

---

17 Cfr. PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 165, e também em "Apreensão de correio electrónico em Processo Penal", *in* Revista do Ministério Público, *passim*, MOURAZ LOPES, Garantia Judiciária no Processo Penal, p. 43, PEDRO DIAS VENÂNCIO, Breve introdução da questão da investigação e meios de prova na criminalidade informática, pp. 22-23, e Acórdãos da Relação de Lisboa de 13/10/2004 e 15/07/2008 e da Relação de Coimbra de 29/03/2006, *in www.dgsi.pt*.

18 CARLOS ADÉRITO TEIXEIRA, "Escutas Telefónicas: A Mudança de Paradigma e os Velhos e os Novos Problemas", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 283, e PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, pp. 166-168, entendiam que, no caso de mensagens já impressas e que fossem apreendidas em suporte papel, não havia lugar à aplicação do artigo 189.º do Código de Processo Penal, uma vez que, para além de já não se tratar de uma comunicação, os dados de conteúdo não estavam guardados em suporte digital; em tais casos, haveria que aplicar o regime das apreensões. De todo o modo, como refere DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, pp. 90 e ss., não se percebe o porquê de o n.º 1 do artigo 189.º do Código de Processo Penal apenas abranger o armazenamento em suporte digital quando muitos escritos ou imagens em suporte papel podem apresentar características idênticas aos guardados em suporte digital no que diz respeito às relações de confiança comunicacional.

Em primeiro lugar, uma comunicação é, por natureza, uma realidade dinâmica (tratando-se de um processo comunicacional, que vai de um lado ao outro, desde o emissor ao recetor) e não estática e, como tal, não poderá estar guardada; quando muito, o que poderá estar guardado é o seu registo ou o seu produto[19].

Em segundo lugar, uma vez chegada a comunicação à "esfera de domínio" do destinatário, o processo comunicacional extingue-se e os dados de conteúdo da comunicação ficam armazenados como qualquer outro documento (no caso do correio eletrónico, o ficheiro do *e-mail* recebido é, em tudo, semelhante a um qualquer outro ficheiro guardado no computador, devendo ser tratado como um mero documento[20]), sendo, por isso, apreendidos e não intercetados[21].

Em terceiro lugar, o regime também era aplicável a comunicações já "abertas" (*i.e.* cujo conteúdo já é do conhecimento do destinatário[22]), ou seja, num momento em que já não existe qualquer tutela no âmbito do direito à inviolabilidade da correspondência e de outros meios de comunicação privada, pois já não se está naquela "específica situação de perigo" e de carência de tutela da proteção constitucional deste direito fundamental de que fala COSTA ANDRADE; ora, daqui resultava a manutenção do sigilo das comunicações *ad aeternum*, de que resultava uma enorme disfuncionalidade entre regimes paralelos (o regime das apreensões e o regime da intervenção nas comunicações)[23], que, por motivos óbvios, é de evitar ao máximo.

Em quarto lugar, este regime criava enormes dificuldades operacionais de implementação perfeitamente evitáveis e que podiam ter graves repercussões (negativas) ao nível da investigação criminal[24]. Assim, se, no decurso de uma busca, fosse apreendido um

19 Cfr. PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 164, e também em "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, p. 121, e SANTOS CABRAL, "Art. 189º", *in* Código de Processo Penal, pp. 835-836.

20 Assim, COSTA ANDRADE, "Art. 194.º", *in* Comentário Conimbricense, I, 2.ª Edição, p. 1097, SANTOS CABRAL, "Art. 189º", *in* Código de Processo Penal, pp. 835-836, e PEDRO VERDELHO, "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, p. 121.

21 Cfr. PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 164, e SANTOS CABRAL, "Art. 189º", *in* Código de Processo Penal, pp. 835-836.

22 E, como tal, perfeitamente similar a uma carta já aberta e lida pelo destinatário, em que já não se aplica o regime da apreensão da correspondência.

23 Cfr. PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 165, e também em "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, p. 122.

24 Assim, COSTA ANDRADE, "Bruscamente no Verão Passado", pp. 185-186, PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 165, e também em "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, p. 123, ANDRÉ LAMAS LEITE, "Entre Péricles e Sísifo: o novo regime legal das escutas telefónicas", *in* Revista

computador, no qual estivessem guardadas mensagens de correio eletrónico, haveria que solicitar ao Juiz de Instrução Criminal autorização para proceder à "leitura" dessas mensagens, o que, implicando alguma perda de tempo entre o momento em que a apreensão era feita e o momento em que o acesso fosse autorizado, poderiam ocorrer perdas graves ao nível da eficácia da investigação.

Com a entrada em vigor da Lei n.º 109/2009, de 15 de setembro, o legislador optou por, no artigo 17.º, determinar a aplicação do regime da apreensão de correspondência à apreensão de correio eletrónico e registos de comunicação de natureza semelhante, sancionando a equiparação do correio eletrónico ao correio tradicional e abandonando a equiparação às escutas telefónicas que tinha operado no Código de Processo Penal. Contudo, apesar da entrada em vigor da Lei n.º 109/2009, de 15 de setembro, a redação do n.º 1 do artigo 189.º do Código de Processo Penal manteve-se inalterada. De todo o modo, consideramos que o n.º 1 do artigo 189.º do Código de Processo Penal, na parte em que se refere a correio eletrónico e aos registos de comunicação de natureza semelhante foi tacitamente revogado pelos artigos 17.º e 18.º da Lei n.º 109/2009, de 15 de setembro, pelo que o legislador optou por abandonar a equiparação da apreensão de correio eletrónico às escutas telefónicas.

Esta opção do legislador não corresponde à transposição de qualquer norma da Convenção sobre o Cibercrime[25], sendo uma criação do legislador português ao abrigo da sua liberdade de conformação. De seguida, analisaremos criticamente esta opção legislativa.

6. DA DESADEQUAÇÃO DA EQUIPARAÇÃO DO CORREIO ELETRÓNICO AO CORREIO TRADICIONAL

A primeira reflexão que o aresto em análise nos suscita prende-se com a adequação, ou não, da equiparação do correio eletrónico ao correio tradicional em termos de regime, sendo que a opção legislativa contida no artigo 17.º da Lei n.º 109/2009, de 15 de setembro, ao proceder a tal equiparação, se nos afigura pouco acertada.

Portuguesa de Ciência Criminal, 2007, p. 662, e MAGISTRADOS DO MINISTÉRIO PÚBLICO DO DISTRITO JUDICIAL DO PORTO, Código de Processo Penal, p. 508.

25 Porém, PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 116, considera que o artigo 17.º, conjuntamente com os artigos 15.º e 16.º da Lei n.º 109/2009, engloba-se no artigo 19.º da Convenção sobre o Cibercrime.

Assim, desde logo, a apreensão de correspondência regulada no Código de Processo Penal consiste na retirada do circuito normal do correio[26] do suporte através do qual se efetua uma comunicação postal ou telegráfica, impedindo que chegue ao seu destinatário (e, por isso, o processo comunicacional terá de estar em curso[27]), pelo que restringe o direito à inviolabilidade da correspondência[28]. Por isso, a apreensão da correspondência ainda não enviada pelo remetente, entregando-a de qualquer forma (*v.g.* depositando-a no marco do correio) ao operador do serviço postal não segue o regime especial da apreensão da correspondência[29], pois o processo comunicacional ainda não se iniciou e, como tal, o suporte que corporiza a comunicação não está protegido pelo direito à inviolabilidade da correspondência. E o mesmo se aplica à que já foi recebida pelo destinatário[30].

Ora, diversamente da apreensão de correspondência, a apreensão de correio eletrónico e registos de comunicação de natureza semelhante não se aplica à obtenção, em tempo real, de correio eletrónico, SMS, etc. (que serão obtidos através da interceção de comunicações, regulada no artigo 18.º da Lei n.º 109/2009, de 15 de setembro), mas à obtenção de correio eletrónico, SMS, etc. que já foi recebido pelo destinatário e que estão armazenados no sistema informático que foi legitimamente acedido pelas autoridades. Daí que a apreensão de correio eletrónico e registos de comunicação de natureza semelhante restrinja os direitos à intimidade/privacidade, à palavra virtual e à autodeterminação informacional, mas não o direito à inviolabilidade das comunicações[31]. Na verdade, o direito à inviolabilidade da

26 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, p. 509, e BENJAMIM SILVA RODRIGUES, Das Escutas Telefónicas, II, p. 72.

27 Cfr. DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, p. 117, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 765, e SCHÄFER, "§99", *in* Löwe-Rosenberg Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 2.º Vol., 25.ª Edição, pp. 306 e 309-310.

28 Cfr. ROXIN/SCHÜNEMANN, Strafverfahrensrecht, 27.ª Edição, p. 281, MEYER-GOSSNER, Strafprozessordnung, 56.ª Edição, p. 367, BENJAMIM SILVA RODRIGUES, Das Escutas Telefónicas, II, p. 72, SIMAS SANTOS/LEAL-HENRIQUES, Código de Processo Penal Anotado, Vol. I, 3.ª Edição, p. 1154, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 763, e Acórdãos do Supremo Tribunal de Justiça de 18/05/2006 e da Relação de Lisboa de 20/12/2011, *in www.dgsi.pt*.

29 Cfr. ROXIN/SCHÜNEMANN, Strafverfahrensrecht, 27.ª Edição, p. 283, BENJAMIM SILVA RODRIGUES, Das Escutas Telefónicas, II, p. 72, SCHÄFER, "§99", *in* Löwe-Rosenberg Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 2.º Vol., 25.ª Edição, pp. 306 e 309-310, e CORDERO, Procedura Penale, 8.ª Edição, p. 843.

30 Cfr. COSTA ANDRADE, "Art. 194.º", *in* Comentário Conimbricense, I, 2.ª Edição, p. 1087, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 763, BENJAMIM SILVA RODRIGUES, Da Prova Penal, II, p. 330, RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 187, e EISENBERG, Beweisrecht der StPO, 5.ª Edição, p. 811.

31 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 509 e 542, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, pp. 117-118, COSTA ANDRADE, "Bruscamente no Verão Passado" pp. 159-160, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, pp. 763 e 765, CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 40-41, e Acórdãos da Relação de Lisboa de 02/03/2011, 29/03/2012 e 24/09/2013, da Relação do Porto de 07/07/2010 e 22/05/2013 e da Relação de Guimarães de 15/10/2012, *in www.dgsi.pt*.

correspondência e de outros meios de comunicação privada consiste na proibição de terceiros[32] se intrometerem, tomarem conhecimento, registarem, utilizarem ou divulgarem o conteúdo de comunicações privadas[33] realizadas por qualquer meio[34] que tenham um emissor e um recetor ou círculo de recetores previamente determinado[35], terminando a tutela deste direito fundamental no momento em que o processo comunicacional termina, *i.e.* quando a comunicação chega ao "aparelho terminal" (*Endgerät*) ou é entregue ao destinatário[36].

Assim, ocorrendo a apreensão num momento em que o processo comunicacional já terminou e, como tal, quando já não existe a específica situação de perigo e de carência da proteção constitucional da inviolabilidade das comunicações, a apreensão de correio eletrónico e registos de comunicação de natureza semelhante não restringe o direito à inviolabilidade da correspondência e de outros meios de comunicação privada. E, por isso, não se justifica a sujeição de um meio de obtenção de prova que não configura qualquer intromissão num processo comunicacional alheio ao regime de um meio de obtenção de prova cuja utilização passa precisamente por uma tal intromissão.

Também não vemos em que medida o correio eletrónico já recebido será diferente de outros dados informáticos (*v.g.* ficheiros contendo documentos resultantes de um processador

32 Daí que quando um dos interlocutores da conversação ou comunicação grava a mesma ou conta às autoridades aquilo que ouviu dizer ao outro interlocutor não ocorre nenhuma lesão deste direito (cfr. COSTA ANDRADE, "Bruscamente no Verão Passado" pp. 158-159, sendo que a inviolabilidade das comunicações nada tem a ver com a garantia de que o outro interlocutor mantenha reserva sobre o conteúdo da comunicação, o que, por sua vez, nada tem a ver com a inviolabilidade da correspondência e de outros meios de comunicação (cfr. COSTA ANDRADE, *Op. e Loc. Cit.*).

33 GOMES CANOTILHO/VITAL MOREIRA, Constituição Anotada, I, 4.ª Edição, pp. 544-546.

34 Cfr. GERMANO MARQUES DA SILVA/FERNANDO SÁ, "Art. 34.º", *in* Constituição Anotada, I, 2.ª Edição, p. 772. Assim, incluem-se aqui os mais sofisticados meios de comunicação de mensagens e os respetivos dados eletrónicos (cfr. JARASS/PIEROTH, Grundgesetz Kommentar, pp. 305-306, CONDE CORREIA, "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32.º, n.º 8, 2.ª parte, da CRP)?", *in* Revista do Ministério Público, n.º 79, p. 51, DORSCH, Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, p. 7, GONZÁLEZ-CUÉLLAR SERRANO, "Garantías constitucionales de la persecución penal en el entorno digital", *in* Prueba y Proceso Penal, p. 165, e Acórdão Wieser e Bicos Beteiligungen GmbH c. Áustria do TEDH, *in www.echr.coe.int*).

35 Cfr. GOMES CANOTILHO/VITAL MOREIRA, Constituição Anotada, I, 4.ª Edição, p. 544, GERMANO MARQUES DA SILVA/FERNANDO SÁ, "Art. 34.º", *in* Constituição Anotada, I, 2.ª Edição, p. 772, e Acórdãos do Tribunal Constitucional n.º 403/2015, *in www.tribunalconstitucional.pt*, do Supremo Tribunal de Justiça de 03/03/2010 e da Relação do Porto de 22/05/2013 e 03/12/2013, *in www.dgsi.pt*.

36 Cfr. PINTO DE ALBUQUERQUE, Comentário do Código de Processo Penal, 4.ª Edição, pp. 509 e 542, FRIGOLS I BRINES, "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", *in* La Protección Jurídica de la Intimidad, pp. 55 e 62 e ss., SCHROEDER, Strafprozessrecht, 4.ª Edição, p. 82, BÄR, TK-Überwachung, p. 36, DURNER, "Art. 10", *in* Maunz-Dürig Grundgesetz Kommentar, II, pp. 47-48 e 52, Acórdãos da Relação de Lisboa de 02/03/2011, da Relação do Porto de 03/04/2013, 24/04/2013, 22/05/2013 e 03/12/2013 e da Relação de Coimbra de 02/03/2005, *in www.dgsi.pt*, e Sentença do *Grosse Senat für Strafsachen do Bundesgerichtshof* de 13/05/1996, *in* BGHSt, 42, pp. 139 e ss.

de texto, folha de cálculo ou de um programa para criação ou apresentação digital de *slides*[37]), cuja apreensão ocorre à luz do regime do artigo 16.º da Lei n.º 109/2009) e que também poderão incluir informações de cariz privado ou até íntimo, não se percebendo o porquê de o Ministério Público poder autorizar a apreensão de correspondência ou de uma cópia em suporte papel de um *e-mail* guardado num cofre e ser necessária autorização do Juiz de Instrução Criminal para se apreender um *e-mail* guardado num computador[38].

Nem podemos olvidar que poderão estar armazenados no sistema informático outros dados informáticos de conteúdo muito mais sensível, em termos de intimidade/privacidade, do que as mensagens de correio eletrónico e, no entanto, o legislador optou por submeter a sua apreensão à disciplina do artigo 16.º da Lei n.º 109/2009, de 15 de setembro, considerando que o mecanismo previsto no n.º 3 desse preceito é suficiente para a salvaguarda do direito à intimidade/privacidade e do direito à autodeterminação informacional. De resto, nos casos previstos no n.º 3 do artigo 16.º da Lei n.º 109/2009, de 15 de setembro, a intervenção do Juiz apenas poderá ocorrer *a posteriori* do conhecimento desses dados informáticos pelo órgão de polícia criminal (pois só o seu conhecimento poderá levar a concluir que contém dados pessoais ou íntimos e que, como tal, a sua junção aos autos terá de ser judicialmente autorizada), pese embora se possa tratar de dados de cariz muito mais sensível do que muitas, porventura a maioria das mensagens de correio eletrónico.

E a aplicação do regime da apreensão de correspondência gera uma descontinuidade, em termos de regime legal, entre a correspondência física aberta e lida pelo destinatário e o correio eletrónico recebido e lido pelo destinatário, pois, após ser recebida, a correspondência física torna-se num mero documento e está sujeita a apreensão nos termos gerais, ao passo que a apreensão do correio eletrónico continua sujeita ao regime muito mais garantístico da apreensão de correspondência[39]. E será certamente por isso que, a fim de minimizar os efeitos nefastos da opção legislativa, não falta quem, considerando que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, deverá ser interpretado de forma hábil, entenda que a remissão para o regime da apreensão de correspondência só deverá ter lugar nos casos em que o *e-mail*, SMS, MMS, etc., apesar de já recebidos, ainda não tenham sido abertos pelo destinatário, como sucede com a correspondência (que, uma vez aberta pelo destinatário, poderá ser apreendida

37 Cfr. ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, p. 209.
38 Cfr. CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, p. 41.
39 Cfr. RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 277.

nos termos gerais como qualquer outro documento e não à luz do artigo 179.º do Código de Processo Penal)[40], entendimento que subscrevemos *de jure condito*. E, do mesmo modo, subscrevemos o entendimento de SANTOS CABRAL quando afirma que, «*A mensagem recebida em telemóvel, atenta a natureza e finalidade do aparelho e o seu porte pelo arguido no momento da revista, é de presumir que, uma vez recebida, foi lida pelo seu destinatário*»[41].

E, para além de não se justificar aplicar um meio de obtenção de prova que configura uma intervenção nas comunicações a uma situação em que inexiste qualquer intervenção nas comunicações, não podemos olvidar que, no plano das consequências, tal opção do legislador acaba por gerar enormes dificuldades à investigação, quando a finalidade da Lei n.º 109/2009, de 15 de setembro, era (também) simplificar a investigação do Cibercrime.

Assim, do ponto de vista operacional, será extremamente difícil aplicar o regime da apreensão de correspondência à abertura e tomada de conhecimento do teor das comunicações eletrónicas[42], pois, podendo os *e-mails* ser em grande número e apenas alguns terem relevância para a investigação, a sua prévia abertura, leitura e posterior seleção para servirem como prova por parte do juiz tenderá a ser uma tarefa verdadeiramente titânica e, no caso de ocorrer na fase de inquérito, os investigadores (polícias) terão um muito melhor conhecimento da investigação (o que muito auxiliará na hora de selecionar quais os *e-mails* cujo conteúdo é relevante para a investigação) do que o Juiz de Instrução Criminal, que apenas intervém pontualmente[43].

E, se a apreensão ocorrer no local onde estão guardados os dados, os investigadores teriam de, à cautela, ser acompanhados pelo Juiz de Instrução Criminal ou, logo que detetassem a existência de correio eletrónico, teriam de contactar o Juiz de Instrução Criminal para este se deslocar ao local ou teriam de apreender e transportar os computadores, para o Juiz de Instrução Criminal poder visionar os *e-mails*, o que, em termos logísticos é dificilmente exequível. De resto, na medida em que a apreensão terá lugar na sequência de uma pesquisa informática ou

40 PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 509 e 542, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, pp. 117-118, COSTA ANDRADE, "Bruscamente no Verão Passado" pp. 159-160, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, pp. 763 e 765, CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 40-41, e Acórdãos da Relação de Lisboa de 02/03/2011 e 24/09/2013, e da Relação de Guimarães de 15/10/2012, *in www.dgsi.pt*; contra, Acórdãos da Relação do Porto de 12/09/2012 e da Relação de Guimarães de 29/03/2011, *in www.dgsi.pt*.

41 SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 765.

42 Cfr. RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, pp. 185 e 275.

43 Daí que, neste ponto, o regime do artigo 17.º da Lei n.º 109/2009, de 15 de setembro, seja ainda mais nocivo para a investigação do que o regime das escutas telefónicas, tendo em conta o disposto nos n.ºs 1 a 5 do artigo 188.º do Código de Processo Penal.

de outro acesso legítimo a um sistema informático[44] e porque o modo habitual de apreensão dos dados informáticos existentes num sistema informático no decurso dessa diligência é realizando um "clone" do suporte que contém esses dados, sendo que a ferramenta forense utilizada não irá distinguir entre mensagens de correio eletrónico e outros dados informáticos e só quando o perito procede à análise dos dados apreendidos é que deparará com as mensagens de correio eletrónico[45]. E essa circunstância é claramente visível na situação *sub juditio* no aresto de cuja análise nos ocupamos, em que a cópia dos dados existentes no sistema informático foi realizada logo no dia em que a pesquisa foi realizada (24/03/2017) e a extração/gravação dos dados que respeitavam a mensagens de correio eletrónico apenas foi realizada no dia 18/08/2017, certamente quando se procedeu à análise dos dados apreendidos.

Igualmente do ponto de vista técnico, também não se justifica equiparar o correio eletrónico a realidades análogas à correspondência "tradicional". Na verdade, fruto da sua natureza digital, a abertura de um *e-mail* nada tem a ver com a abertura de um sobrescrito contendo uma carta[46] e a cifra nada tem a ver com um envelope ou outro invólucro corpóreo[47], sendo que, no plano estritamente técnico, um *e-mail* jamais poderá ser equiparado à correspondência "tradicional"[48], como demonstram à saciedade aspetos como a filtragem de mensagens, a possibilidade de envio em massa de mensagens de correio eletrónico, as mensagens recebidas (e abertas) por engano ou as mensagens privadas enviadas através de *Webmail*[49]. O correio eletrónico não utiliza as redes postais públicas, mas serviços de comunicações eletrónicas acessíveis ao público. Do mesmo modo, atento o elenco de realidades que podem ser objeto de apreensão de correspondência (cartas, encomendas, valores, telegramas), o artigo 179.º do Código de Processo Penal está claramente pensado para

44 A que poderemos subsumir a recolha dos dados informáticos por um especialista no local onde se encontra o sistema informático ou o suporte autónomo, a busca "tradicional" ou a revista (nos termos dos artigos 174.º e ss. do Código de Processo Penal) ou o acesso ao sistema informático ou ao suporte autónomo por via de uma injunção para apresentação ou concessão do acesso a dados (cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 118, e DAVID RAMALHO, Métodos Ocultos de Investigação Criminal em Ambiente Digital, pp. 133-134).

45 Cfr. ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, p. 94.

46 Cfr., entre outros, COSTA ANDRADE, "Bruscamente no Verão Passado" p. 159, BENJAMIM SILVA RODRIGUES, Das Escutas Telefónicas, II, pp. 341 e ss., ARMANDO RAMOS, "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, p. 56 (nota 21), e também em A prova digital em processo penal: O correio eletrónico, pp. 47 e ss., e ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, *passim*.

47 Cfr. ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, p. 212.

48 *Vide* os argumentos de caráter técnico aduzidos por ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, pp. 214 e ss., e ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, pp. 58 e ss.

49 Cfr. ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, pp. 56 e ss.

a apreensão de realidades físicas e não virtuais[50] e não nos parece que, após ter sido visionado e considerado irrelevante para a investigação, o correio eletrónico possa ser restituído na verdadeira aceção da palavra ao destinatário (que poderá aceder-lhe sem necessidade de restituição e independentemente de ter sido alvo de apreensão)[51]. De resto, em termos de específica situação de perigo e de carência da proteção constitucional da inviolabilidade das comunicações, ao contrário do que sucede com a correspondência física, o destinatário, ao receber a mensagem, pode dispor de meios de autodefesa para se proteger de infiltrações de terceiros, como a instalação de sistemas de segurança, programas antivírus, codificação críptica, *firewalls* ou o apagamento ou a destruição dos dados, que nada têm a ver com uma caixa de correio equipada com fechadura, sendo que, no caso do correio eletrónico, só poderá ser recebido por via de um sistema informático que poderá estar equipado com os mencionados dispositivos, ao passo que o correio tradicional até poderá ser entregue em mão a um terceiro que, depois, o entregará ao destinatário.

Por isso, *de jure condendo*, a apreensão de correio eletrónico e comunicações de natureza semelhante deveria ocorrer à luz do artigo 16.º da Lei n.º 109/2009, de 15 de setembro (constituindo o seu n.º 3 salvaguarda suficiente em matéria de correio eletrónico e realidades análogas), pois já não nos encontramos no âmbito de um processo comunicacional[52]. De todo o modo, como referimos, mesmo *de jure condito*, a fim de minimizar os efeitos nefastos da opção legislativa, entendemos que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, deverá ser interpretado de forma hábil, só se aplicando o regime da apreensão de correspondência nos casos em que o *e-mail*, SMS, MMS, etc., apesar de já recebido, ainda não tenha sido aberto pelo destinatário, sendo de presumir que, uma vez recebido, já foi lido pelo seu destinatário.

50 Cfr. RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 185, que refere que, em face dos exemplos dados pelo legislador, a "qualquer outra correspondência" não incluirá realidades meramente virtuais.
51 Cfr. RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 185.
52 No mesmo sentido, ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, p. 113.

7. TODOS OS ASPETOS DO REGIME DA APREENSÃO DE CORRESPONDÊNCIA DEVERÃO SER APLICADOS, E NOS MESMOS TEMPOS, À APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÃO DE NATUREZA SEMELHANTE?

A segunda reflexão que o aresto sob análise suscita é relativa à questão de saber se a remissão que artigo 17.º da Lei n.º 109/2009, de 15 de setembro, opera para o regime da apreensão da correspondência previsto no Código de Processo Penal abrange todos os aspetos desse regime e se tal regime deverá ser aplicado à apreensão de correio eletrónico e registos de comunicação de natureza semelhante nos mesmos termos em que se aplica à apreensão da correspondência "tradicional".

Antes de entrarmos na análise da questão, desde já diremos que, pelas grandes diferenças entre a correspondência "tradicional" e o correio eletrónico que elencámos (e que desaconselham qualquer equiparação em termos de regime jurídico), essa remissão deverá ser sempre lida *cum grano salis* e *mutatis mutandis*.

Assim, no que tange à competência autorizativa, ainda que a remissão não a abranja (pois a autorização judicial é expressamente referida no artigo 17.º da Lei n.º 109/2009, de 15 de setembro), no caso da apreensão de correspondência, a autorização terá de ser prévia à realização da diligência, o que será sempre possível, dado que a diligência é especificamente dirigida à apreensão da correspondência. Diversamente, no caso da apreensão de correio eletrónico e registos de comunicação de natureza semelhante, a apreensão tem lugar na sequência de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, que, no inquérito, são autorizados pelo Ministério Público, sendo que não se sabe se, na sequência dessa pesquisa ou acesso serão apreendidos mensagens de correio eletrónico ou registos de comunicação de natureza semelhante ou se apenas serão apreendidos dados informáticos de outro tipo (submetidos ao regime do artigo 16.º da Lei n.º 109/2009, de 15 de setembro, sendo que a intervenção do Juiz prevista no n.º 3 desse preceito apenas ocorre após a apreensão e terem sido detetados dados de cariz pessoal ou íntimo).

Para além disso, o modo habitual de apreensão dos dados informáticos existentes num sistema informático no decurso dessa diligência é realizando um "clone" do suporte que contém esses dados, sendo que a ferramenta forense utilizada não irá distinguir entre mensagens de correio eletrónico e outros dados informáticos e só quando o perito procede à análise dos dados

apreendidos é que deparará com as mensagens de correio eletrónico[53], pelo que só nesse momento as autoridades serão confrontadas com a necessidade da autorização judicial (situação em tudo similar à prevista no n.º 3 do artigo 16.º da Lei n.º 109/2009, de 15 de setembro).

Por isso, consideramos que a autorização do Juiz só poderá ser concedida *a posteriori* face à chegada das mensagens ao conhecimento de quem conduz a investigação[54].

Do mesmo modo, no caso da apreensão de correspondência, nos termos do n.º 3 do artigo 179.º do Código de Processo Penal, se a correspondência não for relevante para a prova, deverá ser restituída, pelo que a carta, encomenda, etc. entregues ao seu legítimo destinatário. Diversamente, no caso da apreensão de correio eletrónico e registos de comunicação de natureza semelhante, fruto das evidentes diferenças face à correspondência "tradicional", não será possível dar cumprimento à parte final do disposto no aludido n.º 3 do artigo 179.º do Código de Processo Penal quanto à restituição[55], embora o juiz fique vinculado a guardar segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova.

Para além disso, na apreensão de correspondência, nos termos do n.º 3 do artigo 179.º do Código de Processo Penal, juiz terá de ser a primeira pessoa a tomar conhecimento do conteúdo da correspondência; diversamente, no caso da apreensão de correio eletrónico e registos de comunicação de natureza semelhante o juiz não terá de ser (nem poderia ser) a primeira pessoa a tomar conhecimento das mensagens de correio eletrónico ou realidades análogas (embora seja quem decide da junção, ou não, das mensagens ao autos)[56]. Na verdade, sem prejuízo de os investigadores deverem ter especiais cuidados para não tomarem conhecimento do conteúdo das comunicações sem que o Juiz o faça em primeiro lugar, pode muito bem suceder que uma mensagem de correio eletrónico tenha sido guardada como um documento de outra natureza (*v.g.* como documento de *MSWord*) e não como um ficheiro de correio eletrónico e só quando o perito que procede ao exame abre o ficheiro é que se apercebe de que se trata de um *e-mail*, sendo que, num tal caso, não faz sentido considerar a prova nula.

53 Cfr. ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, p. 94.
54 Cfr. PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* Scientia Ivridica, Tomo LVIII, p. 743, e DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 153.
55 No mesmo sentido, RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 275.
56 No mesmo sentido, PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* ScIvr, T. LVIII, pp. 744-745.

E também não podemos deixar de ter em conta que, no caso da interceção de correio eletrónico e comunicações similares em tempo real, em que existe inclusivamente uma intervenção nas comunicações (sendo, por isso, muito mais gravoso do que no caso da apreensão desses dados após terem sido recebidos pelo destinatário), nos termos dos n.ºs 1 a 5 do artigo 188.º do Código de Processo Penal, aplicável *ex vi* do n.º 4 do artigo 18.º da Lei n.º 109/2009, de 15 de setembro, quem primeiro toma conhecimento do teor dessas comunicações é o órgão de polícia criminal, seguidamente o magistrado do Ministério Público e só depois é que o Juiz toma conhecimento. Ademais, no caso da apreensão de dados informáticos que incida sobre dados íntimos/privados ou pessoais (que terão um conteúdo mais sensível do que muitas mensagens de correio eletrónico), o Juiz apenas toma conhecimento do conteúdo depois de os órgãos de polícia criminal o terem feito. E, se assim é num caso em que existe uma restrição de direitos fundamentais muito mais intensa e a exigência de ser o Juiz a tomar primeiro conhecimento do teor da correspondência ("tradicional") radica na necessidade de uma mais intensa tutela de direitos fundamentais, não nos repugnaria que o artigo 17.º Lei n.º 109/2009, de 15 de setembro, pudesse ser alvo de uma interpretação hábil, no sentido de a exigência de ser o Juiz o primeiro a tomar conhecimento do teor da correspondência "tradicional", nos termos do n.º 3 do artigo 179.º do Código de Processo Penal, não ser aplicável à apreensão de mensagens de correio eletrónico ou de registos de comunicações de natureza semelhante, com evidentes ganhos em termos operacionais e sem maior detrimento para a tutela de direitos fundamentais.

No que tange às medidas cautelares e de polícia, como vimos, por força da remissão do artigo 17.º da Lei n.º 109/2009, de 15 de setembro, para o regime da apreensão de correspondência do Código de Processo Penal, será possível aplicar o artigo 252.º deste Código em sede de apreensão de correio eletrónico e registos de comunicação de natureza semelhante[57]. Contudo, pela especificidade do correio eletrónico face ao correio tradicional, não nos parece que a medida cautelar e de polícia prevista no n.º 2 do artigo 252.º do Código de Processo Penal possa ser aplicada à apreensão de correio eletrónico e registos de comunicação de natureza semelhante[58]. Com efeito, tal medida não está prevista para qualquer

57 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Ed., p. 510, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, p. 118, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 765, e Acórdãos da Relação de Lisboa de 11/01/2011 e 06/02/2018, *in www.dgsi.pt*; contra, ARMANDO RAMOS, "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, pp. 56-57.
58 Contra, Acórdão da Relação de Lisboa de 06/02/2018, *in www.dgsi.pt*.

forma de correspondência, mas apenas para encomendas e valores fechados, sendo que, no âmbito correio eletrónico e dos registos de comunicação semelhantes, inexiste qualquer modalidade que possa ser equiparada a tais realidades, mas tão-só a cartas, telegramas ou realidades análogas. Deste modo, pela restrição às encomendas e valores fechados, a medida cautelar e de polícia prevista no n.º 2 do artigo 252.º do Código de Processo Penal não poderá ser aplicada à apreensão de correio eletrónico e registos de comunicação de natureza semelhante.

Mas já será possível aplicar a medida cautelar e de polícia prevista no n.º 3 do artigo 252.º do Código de Processo Penal, contanto que tal seja tecnicamente viável, ordenando o órgão de polícia criminal ao fornecedor de serviço a não remessa do correio eletrónico, das SMS, etc., para o destinatário, devendo a ordem ser convalidada pelo Juiz de Instrução Criminal, mediante despacho fundamentado, no prazo de 48 horas e, caso tal não suceda, a ordem de suspensão fica sem efeito e o correio eletrónico ou realidade análoga são remetidos ao destinatário.

Deste modo, consideramos que o regime da apreensão da correspondência previsto no Código de Processo Penal deverá ser aplicado *cum grano salis* e *mutatis mutandis* à apreensão de correio eletrónico e registos de comunicação de natureza semelhante, existindo aspetos do regime da apreensão da correspondência que não são aplicáveis à apreensão de correio eletrónico e registos de comunicação de natureza semelhante ou, sendo-o, não o são nos mesmos termos em que são aplicáveis à apreensão de correspondência "tradicional".

8. CONCLUSÕES

i. O Tribunal da Relação de Lisboa, no seu Acórdão de 6 de fevereiro de 2018 (Processo 1950/17.0 T9LSB-A.L1-5), considerou que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, remete expressamente para o regime da apreensão de correspondência previsto no Código de Processo Penal, sem redução do seu âmbito, impondo-se, por isso, a aplicação de tal regime na sua totalidade;

ii. As vantagens proporcionadas pelas novas tecnologias tanto podem ser aproveitadas para fins lícitos como para fins ilícitos;

iii. Os criminosos utilizam as novas tecnologias da informação e comunicação para preparar ou executar crimes, bem como para suprimir as provas do seu cometimento, usufruindo da rapidez, anonimato e volatilidade das novas formas de comunicação à distância, que dificultam de sobremaneira a sua deteção e, quando sejam utilizadas medidas antiforenses, a sua interceção e gravação;

iv. O correio eletrónico é «*qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha*».

v. O artigo 17.º da Lei n.º 109/2009, de 15 de setembro, equipara o correio eletrónico e as comunicações de natureza semelhante (SMS e MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via *Whatsapp*, *Viber*, *Skype*, *Facebook*, etc.) ao correio tradicional;

vi. Pelas enormes diferenças existentes entre o correio eletrónico e o correio tradicional, bem como pelas disfunções que gera em termos de regime jurídico e pelas dificuldades operacionais que a aplicação do regime da apreensão de correspondência suscita, não se justifica equiparar o correio eletrónico ao correio tradicional;

vii. O artigo 17.º da Lei n.º 109/2009, de 15 de setembro, deveria ser revogado, passando a aplicar-se à apreensão de correio eletrónico e comunicações de natureza semelhante o regime artigo 16.º dessa Lei (constituindo o seu n.º 3 salvaguarda suficiente para a proteção da intimidade/privacidade);

viii. *De jure condito*, a fim de minimizar os efeitos nefastos da opção legislativa, o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, deverá ser interpretado de

forma hábil, apenas sendo aplicável nos casos em que o *e-mail*, SMS, MMS, etc., ainda não tenham sido abertos pelo destinatário;

ix. A medida cautelar e de polícia prevista no n.º 3 do artigo 252.º do Código de Processo Penal é aplicável à apreensão de correio eletrónico e registos de comunicação de natureza semelhante, mas o mesmo não acontece com a medida prevista no n.º 2 desse preceito;

x. O regime da apreensão da correspondência previsto no Código de Processo Penal deverá ser aplicado *cum grano salis* e *mutatis mutandis* à apreensão de correio eletrónico e registos de comunicação de natureza semelhante, existindo aspetos do regime da apreensão da correspondência que não são aplicáveis à apreensão de correio eletrónico e registos de comunicação de natureza semelhante ou, sendo-o, não o são nos mesmos termos em que são aplicáveis à apreensão de correspondência "tradicional".

BIBLIOGRAFIA

Abadinsky, Howard – Organized Crime, 9.ª Edição, Wadsworth Cengage Learning, Belmont, 2007.

Albanese, Jay S. – Organized Crime in Our Times, 5.ª Edição, Matthew Bender & Company, Newark, 2007.

Albuquerque, Paulo Pinto de – Comentário ao Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica Editora, 4.ª Edição, Lisboa, 2011.

Andrade, Manuel da Costa – "Bruscamente no Verão Passado", a reforma do Código de Processo Penal, Observações críticas sobre uma Lei que podia e devia ter sido diferente, Coimbra Editora, Coimbra, 2009.

Andrade, Manuel da Costa – "Art. 194º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, 2.ª Edição, pp. 1080 e ss., Coimbra Editora, Coimbra, 2012.

Bär, Wolfgang – TK-Überwachung, §§100a-101 StPO mit Nebengesetzen Kommentar, Carl Heymanns Verlag, Colónia e Munique, 2010.

Bravo, Rogério – "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, pp. 207 e ss., Coimbra Editora, Coimbra, 2006.

Cabral, José António Santos – "Art. 179º", *in* Código de Processo Penal Comentado, pp. 762 e ss., Almedina, Coimbra, 2014.

Cabral, José António Santos – "Art. 189º", *in* Código de Processo Penal Comentado, pp. 833 e ss., Almedina, Coimbra, 2014.

Canotilho, José Joaquim Gomes /Moreira, Vital – Constituição da República Portuguesa Anotada, Volume I, 4.ª Edição, Coimbra Editora, Coimbra, 2007.

Conselho da Europa – Relatório Explicativo da Convenção sobre o Cibercrime, *in https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf* (pesquisa em 06/06/2018).

Correia, João Conde – "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32.º, n.º 8, 2.ª parte, da CRP)?", *in* Revista do Ministério Público, n.º 79, pp. 45 e ss., Lisboa, 1999.

Correia, João Conde – "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 29 e ss., Lisboa, 2014.

Dorsch, Claudia – Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, Duncker&Humblot, Berlim, 2005.

Durner, Wolfgang – "Art. 10", *in* Maunz-Dürig Grundgesetz Kommentar, Volume II (Art. 6-15), Fascículo 57 (Janeiro de 2010), pp. 1 e ss., Verlag C.H.Beck, Munique, 2010.

Eisenberg, Ulrich – Beweisrecht der StPO, 5.ª Edição, Spezialkommentar, C.H.Beck Verlag, Munique, 2006.

Frigols I Brines, Eliseu – "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", *in* La Protección Jurídica de la Intimidad, pp. 37 e ss., Iustel, Madrid, 2010.

Glenny, Misha – Darkmarket, Como os Hackers se tornaram a nova Máfia, Civilização, Lisboa, 2012.

González-Cuéllar Serrano, Nicolás – "Garantías constitucionales de la persecución penal en el entorno digital", *in* Prueba y Proceso Penal, Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado, pp. 149 e ss., Tirant lo blanch, Valência, 2008.

Gutiérrez Francés, Mariluz – "Las altas tecnologías de la información al servicio del blanqueo de capitales transnacional", *in* Blanqueo de Dinero y Corrupción en el Sistema Bancario, Delitos Financieros, Fraude y Corrupción en Europa, Vol. II, pp. 193 e ss., Ediciones Universidad de Salamanca, Salamanca, 2002.

Jarass, Hans D./Pieroth, Bodo – Grundgesetz für die Bundesrepublik Deutschland Kommentar, 11.ª Edição, Verlag C.H. Beck, Munique, 2011.

Leite, André Lamas – "Entre Péricles e Sísifo: O Novo Regime Legal das Escutas Telefónicas", *in* Revista Portuguesa de Ciência Criminal, Ano 17, Fascículo 4.º, pp. 613 e ss., Coimbra Editora, Coimbra, 2007.

Lopes, José Mouraz – Garantia Judiciária no Processo Penal, Do Juiz e da Instrução, Coimbra Editora, Coimbra, 2000.

Magistrados do Ministério Público do Distrito Judicial do Porto – Código de Processo Penal, Comentários e Notas Práticas, Coimbra Editora, Coimbra, 2009.

Mesquita, Paulo Dá – Processo Penal, Prova e Sistema Judiciário, Coimbra Editora, Coimbra, 2010.

Meyer-Gossner, Lutz – Strafprozessordnung mit GVG und Nebengesetzen, 56.ª Edição, Verlag C.H.Beck, Munique, 2013.

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, Coimbra, 2011.

Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, Gestlegal, Coimbra, 2018.

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

Ramos, Armando Dias – A prova digital em processo penal: O correio eletrónico, Chiado Editora, Lisboa, 2014.

Ramos, Armando Dias – "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, pp. 49 e ss., Almedina, Coimbra, 2016.

Rodrigues, Benjamim Silva – Das Escutas Telefónicas À Obtenção da Prova [em Ambiente Digital], Tomo II, Coimbra, 2008.

Rodrigues, Benjamim Silva – Da Prova Penal, Tomo II, Bruscamente…A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, 1.ª Edição, Rei dos Livros, Lisboa, 2010.

Roxin, Claus/Schünemann, Bernd – Strafverfahrensrecht, 27.ª Edição, C.H.Beck, Munique, 2012.

Schäfer, Gerhard – "§99", *in* Löwe-Rosenberg Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 2.º Volume, 25.ª Edição, pp. 303 e ss., De Gruyter, Berlim, 2004.

Schroeder, Friedrich-Christian – Strafprozessrecht, 4.ª Edição, CH Beck, Munique, 2007.

Silva, Germano Marques da /Sá, Fernando – "Art. 34.º", *in* Constituição Portuguesa Anotada, Tomo I, 2.ª Edição, pp. 755 e ss., Coimbra Editora, Coimbra, 2010.

Simas Santos, Manuel/Leal-Henriques, Manuel – Código de Processo Penal Anotado, Volume I, 3.ª Edição, Editora Rei dos Livros, Lisboa, 2008.

Teixeira, Carlos Adérito – "Escutas Telefónicas: A Mudança de Paradigma e os Velhos e os Novos Problemas", *in* Revista do Centro de Estudos Judiciários, Número 9 (Especial), Jornadas sobre a revisão do Código de Processo Penal", pp. 243 e ss., Centro de Estudos Judiciários, Lisboa, 2008.

Venâncio, Pedro Dias – Breve introdução da questão da investigação e meios de prova na criminalidade informática, *in* *www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf* (pesquisa em 14/06/2018).

Venâncio, Pedro Dias – Lei do Cibercrime, Anotada e Comentada, Coimbra Editora, Coimbra, 2011.

Verdelho, Pedro – "Apreensão de correio electrónico em Processo Penal", *in* Revista do Ministério Público, n.º 100, pp. 153 e ss., Lisboa, 2004.

Verdelho, Pedro – "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, pp. 97 e ss., Lisboa, 2006.

Verdelho, Pedro – "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, Número 9 (Especial), Jornadas sobre a revisão do Código de Processo Penal", pp. 145 e ss., Centro de Estudos Judiciários, Lisboa, 2008.

Verdelho, Pedro – "A nova Lei do Cibercrime", *in* Scientia Ivridica, T. LVIII (2009), pp. 717 e ss., Universidade do Minho, Braga, 2009.

JURISPRUDÊNCIA

Tribunal Europeu dos Direitos do Homem

Acórdão Wieser e Bicos Beteiligungen GmbH c. Áustria (de 16 de outubro de 2007), *in www.echr.coe.int*.

PORTUGAL

Tribunal Constitucional

Acórdão n.º 403/2015, *in www.tribunalconstitucional.pt*.

Supremo Tribunal de Justiça

Acórdão de 18 de maio de 2006 (Processo 06P1394), *in www.dgsi.pt.*

Acórdão de 3 de março de 2010 (Processo 886/07.8PSLSB.L1.S1), *in www.dgsi.pt.*

Tribunal da Relação de Coimbra

Acórdão de 2 de março de 2005 (Processo 3756/04), *in www.dgsi.pt.*

Acórdão de 29 de março de 2006 (Processo 607/06), *in www.dgsi.pt.*

Tribunal da Relação de Évora

Acórdão de 6 de janeiro de 2015 (Processo 6793/11.6TDLSB-A.E1), *in www.dgsi.pt.*

Acórdão de 20 de janeiro de 2015 (Processo 648/14.6GCFAR-A.E1), *in www.dgsi.pt.*

Tribunal da Relação de Guimarães

Acórdão de 29 de março de 2011 (Processo 738/10.0GAPTL-A.G1), *in www.dgsi.pt.*

Acórdão de 15 de outubro de 2012 (Processo 68/10.1GCBRG.G1), *in www.dgsi.pt.*

Tribunal da Relação de Lisboa

Acórdão de 13 de outubro de 2004 (Processo 5150/2005-3), *in www.dgsi.pt.*

Acórdão de 15 de julho de 2008 (Processo 3453/2008-5), *in www.dgsi.pt.*

Acórdão de 11 de janeiro de 2011 (Processo 5412/09.3TDLSB-A.L1-5), *in www.dgsi.pt.*

Acórdão de 2 de março de 2011 (Processo 463/07.3TAALM-A.L1-3), *in www.dgsi.pt.*

Acórdão de 20 de dezembro de 2011 (Processo 36/11.6PJOER-A.L1-5), *in www.dgsi.pt.*

Acórdão de 29 de março de 2012 (Processo 744/09-1S5LSB-A.L1-9), *in www.dgsi.pt.*

Acórdão de 24 de setembro de 2013 (Processo 145/10.9GEALM.L2-5), *in www.dgsi.pt.*

Acórdão de 6 de fevereiro de 2018 (Processo 1950/17.0T9LSB-A.L1-5), *in www.dgsi.pt.*

Tribunal da Relação do Porto

Acórdão de 7 de julho de 2010 (Processo 1978/09.4JAPRT-B.P1), *in www.dgsi.pt.*

Acórdão de 3 de abril de 2013 (Processo 856/11.1PASJM.P1), *in www.dgsi.pt.*

Acórdão de 24 de abril de 2013 (Processo 585/11.6PAOVR.P1), *in www.dgsi.pt.*

Acórdão de 22 de maio de 2013 (Processo 74/07.3PASTS.P1), *in www.dgsi.pt.*

Acórdão de 3 de dezembro de 2013 (Processo 37/12.7TBALJ-A.P1), *in www.dgsi.pt.*

Acórdão de 7 de julho de 2016 (Processo 2039/16.0JAPRT.P1), *in www.dgsi.pt.*

Acórdão de 7 de dezembro de 2016 (Processo 1689/16.4JAPRT-A.P1), *in www.dgsi.pt.*

ALEMANHA

Bundesgerichtshof

Jurisprudência Uniformizada

Sentença do Grosse Senat für Strafsachen de 13 de maio de 1996, *in* Entscheidungen des Bundesgerichtshofes in Strafsachen, 42, pp. 139 e ss., Carl Heymanns Verlag KG, Colónia e Berlim, 1997.