A CONSAGRAÇÃO DE UM NOVO PARADIGMA NA ORDEM JURÍDICA: A DIVISÃO BIPARTIDA DOS DADOS RELATIVOS ÀS COMUNICAÇÕES ELECTRÓNICAS

Joana Leal de Oliveira Geraldo Dias[*]

Abstract: *Firstly, the gathering of evidence by electronic means involved only the analysis of the type of data relating to electronic communications, in accordance with legislative developments, case law and doctrine. However, with the entry into force of the Cybercrime Law, a new paradigm was seen in our legal system, in terms of the type of evidence admissible for access and retrieval, which allowed us to overcome the typological division of data (tripartite), providing a time division (bipartite), which takes into account the moment of access, depending on whether it is stored data or data in transmission, without excluding, in each of the phases, all data related to the communication and subsequent to it, ensuring greater protection of the content of private communication and, in turn, reinforcing the protection of the right to inviolability of communication and privacy, in its aspect of the right to informational self-determination, in terms of articles 34 and 35 of the Portuguese Constitution.*

1. INTRODUÇÃO

A realidade digital obriga o legislador a fazer escolhas que têm implicações na legitimidade e na autoridade da lei, "gerando desafios que ultrapassam as

---

Artigo com origem em Relatório de Mestrado em Ciências Jurídico-Forenses, no âmbito de Direito Penal IV, na Faculdade de Direito da Universidade de Lisboa. Por opção da autora, no presente trabalho não se utiliza o Novo Acordo Ortográfico.

fronteiras das disciplinas e envolvem perspectivas teóricas múltiplas"[1]. Deste modo, o presente trabalho visa dar a conhecer a consagração de um novo paradigma na ordem jurídica, com a entrada em vigor da Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro), que resultou na divisão bipartida dos dados relativos às comunicações electrónicas, cujo problema incide sobre o tipo de dados que legitima o respectivo acesso e obtenção, atendendo ao momento a que se reportam, *mutatis mutandis*.

De acordo com esta problemática, este trabalho encontra-se dividido em duas partes, designadamente, a primeira pretende retratar a tipologia dos dados relativos às comunicações electrónicas para efeitos de acesso e de obtenção, contemplando, por um lado, a evolução legislativa da concepção de dados (divisão tripartida, quadripartida ou bipartida) e por outro, as diversas soluções adoptadas no ordenamento jurídico português, acompanhando o entendimento da doutrina e da jurisprudência quanto à sua tipologia e dos direitos em causa, em função dos quais se procede à ponderação da exigibilidade ou da dispensa de despacho judicial com vista à obtenção. A segunda parte apresenta uma análise crítica das opções legislativas, consoante a perspectiva de alguns autores às Leis n.os 48/2007, 32/2008 e 109/2009, e, por último, a posição pessoal sobre esta temática.

Neste contexto, cumpre esclarecer que na presente exposição far-se-á alusão, em termos gerais, a determinadas disposições processuais constantes da Lei n.º 109/2009, cujo regime não nos compete aprofundar, bem como advertir que a nossa análise não visa enunciar os conceitos legais sobre os vários tipos de dados (visto essa tarefa pertencer ao legislador), cabendo antes, proceder a uma abordagem dos tipos à luz do enquadramento jurídico-normativo a que respeitam.

2. A TIPOLOGIA DOS DADOS RELATIVOS ÀS COMUNICAÇÕES ELECTRÓNICAS PARA EFEITOS DE ACESSO E DE OBTENÇÃO

2.1. A evolução legislativa

a) O Projecto de Lei n.º 271/IX – uma miragem de inovação

Primeiramente, em Janeiro de 2003, o Grupo Parlamentar do Centro Democrático Social – Partido Popular (CDS-PP), apresentou na Assembleia

1 Madison, 2005: 348.

da República o Projecto de Lei n.º 271/IX, designado por *Regime Jurídico da Obtenção de Prova Digital Electrónica na Internet*[2]. Neste Projecto de Lei adoptou-se a terminologia prevista na Convenção do Cibercrime, doravante, CCiber[3], visando garantir a obrigação de conservação dos dados relativos às comunicações por parte dos operadores das telecomunicações e, ainda, o acesso em tempo útil a essa informação pelas autoridades de investigação criminal. O mesmo retomou a *distinção tripartida* entre *dados de base*, de *tráfego* e de *conteúdo*, distinguindo até entre dados de base sujeitos ou não ao regime da confidencialidade, com a nomenclatura subjacente ao primeiro Parecer do Conselho Consultivo da Procuradoria Geral da República (PGR) n.º 16/94, *infra* citado.

Não só não fez qualquer menção aos dados de localização se encontrarem contemplados na categoria dos dados de tráfego[4], contrariamente ao que se sufragava, como também previu uma noção inovadora da categoria dos *dados de base* – a *listagem dos movimentos de comunicações* – passando a respeitar à comunicação em si, não apenas à conexão à rede pelo utilizador, ao consagrar, nos seus artigos n.os 2 e 3, que os dados de tráfego e os dados de base não estão sujeitos ao regime de confidencialidade[5], podendo ser fornecidos aquando solicitados pelas autoridades de polícia criminal ou às entidades judiciárias, quer para efeitos de investigação criminal, como da própria prevenção criminal. Tratando-se de dados de base sujeitos ao regime de confidencialidade, o pedido aos operadores das comunicações electrónicas deveria ser, em princípio, realizado e fundamentado pelas autoridades judiciárias.

---

2 Da *Exposição de Motivos* constava "seja da manipulação fraudulenta de dados com o intuito lucrativo [...] seja da utilização indevida da informação contida em arquivos ou suportes informáticos alheios, [...] Está em causa o tratamento de dados pessoais com vista à respectiva protecção, bem como a protecção de privacidade no sector das comunicações electrónicas", bem como "a reserva da intimidade da vida privada e da vida familiar e o sigilo das comunicações não são os únicos valores que, nestes domínios, importa ao Estado de Direito salvaguardar: [...] pelo uso indevido ddas telecomunicações e pela falta de prevenção do uso ilícito dos meios electrónicos, tarefa da qual os operadores devem partilhar por natureza e necessidade".

3 A Convenção do Cibercrime do Conselho da Europa, adoptada em Budapeste em 23 de Novembro de 2001, é o primeiro trabalho de relevo sobre o crime no ciberespaço.

4 Definindo os *dados de base* como "os dados pessoais relativos à conexão à rede de comunicações, designadamente número, identidade e morada de assinante, bem como a listagem de movimentos de comunicações, e que constituem elementos necessários ao estabelecimento de uma base para a comunicação".

5 Por serem compreendidos como os dados relativamente aos quais o utilizador não tenha manifestamente expressado o desejo de não serem publicitados.

Em suma, este Projecto de Lei revela uma configuração de regime inovador relativamente à visão predominantemente propugnada pela jurisprudência, no sentido de conferir um maior grau de exigência para os dados de tráfego do que para os dados de base, sujeitos ou não ao regime de confidencialidade, dispensando, assim, a intervenção judicial para a obtenção destes elementos de prova, excepto quanto aos dados de conteúdo. No entanto, como entendeu Rita Castanheira Neves[6], o Projecto de Lei n.º 271/IX "foi longe demais no alcance das suas disposições, […] há rígidos limites de proporcionalidade, adequação e necessidade a respeitar e também de que em matéria de restrição de direitos, liberdade e garantias há que salvaguardar o mais possível o princípio de reserva do juiz".

b) A Proposta de Lei n.º 155/IX – uma proposta com os dias contados

Em Outubro de 2004, foi apresentada, pelo Partido Social Democrata (PSD), a Proposta de Lei n.º 155/IX, que aprovava o *Regime de Obtenção da Prova Digital Electrónica*. Este estabelecia uma *distinção quadripartida de dados relacionados com comunicações* electrónicas, na medida em que os *dados de localização* foram autonomizados[7], consagrando-se, igualmente, a definição de *dados de tráfego*, *dados de base* e *dados de conteúdo*, de acordo com uma terminologia quase literal à que constava do Projecto de Lei n.º 271/IX, com algumas variações, nomeadamente em sede de limitação do acesso de dados a um catálogo de crimes (artigo 3.º), tal como ao acesso de dados de base, através do qual se previa um regime que distinguia a *listagem de movimentos de comunicação* juntamente com os dados de base sujeitos ao regime de confidencialidade, dos demais dados de base, ou seja, os que não se encontravam sujeitos a esse mesmo regime, aos quais se aplicava a regra prevista para os *dados de localização* e de *tráfego*. Já no que concerne aos *dados de conteúdo*, esta Proposta de Lei remetia *in totum* para o regime das escutas telefónicas, passando-se a aplicar o catálogo de crimes consagrado no Código de Processo Penal (CPP).

A Comissão Nacional de Protecção de Dados (CNPD) *criticou o facto de se ter adoptado uma classificação dos vários tipos de dados que não respeitou os critérios estabelecidos em instrumentos internacionais* vigentes em matéria de protecção

6 Cf. Neves, 2011: 233.

7 Definidos como "quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica de equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível".

de dados de carácter pessoal tratados e armazenados em ficheiros automatizados[8]. Acresce que esta iniciativa legislativa caducou, por motivos atinentes à queda do Governo Constitucional, por dissolução parlamentar da iniciativa do Presidente da República. (sublinhado nosso)

c) Os Projectos de Lei n.os 240/X e 367/X – o recurso ao passado

Em Março de 2006, o Grupo Parlamentar do PSD retomou a Proposta de Lei *supra* mencionada, no âmbito do XVII Governo de Portugal, apresentando o Projecto de Lei n.º 240/X, com igual denominação e conteúdo da mesma.

Mais tarde, com o intuito de se proceder às alterações legislativas ao CPP, pela Unidade de Missão para a Reforma Penal, o Grupo Parlamentar do CDS-PP retomou o Projecto de Lei apresentado em 2003, propondo o Projecto de Lei n.º 367/X, atribuindo-lhe a mesma denominação e teor do mesmo.

d) A Lei n.º 48/2007, de 29 de Agosto – uma sistematização conceptualmente confusa

Em 2007, foram aprovadas as alterações ao CPP, pela Lei n.º 48/2007, de 29 de Agosto, tendo o debate parlamentar que antecedeu a publicação da mesma, abrangido uma discussão conjunta com os Projectos de Lei n.º 240/X e 367/X. Esta Reforma veio proceder à revogação do artigo 190.º, dando lugar ao actual artigo 189.º, com um novo n.º 2. Finalmente, implementou-se um regime legal quanto ao regime aplicável à obtenção de *dados de tráfego*[9], que exigia agora a obtenção de despacho judicial.

No entanto, o seu regime foi alvo de críticas, nomeadamente, a nível sistemático (inalterada a estrutura de 1987), contemplou a possibilidade de obtenção de prova relativa a todas as comunicações electrónicas *na mesma norma* através da qual opera a extensão do regime das escutas telefónicas ao correio electrónico, aos suportes digitais e à intercepção das conversas ambientais. Ademais, da presente norma, nenhuma referência se retira quanto às disposições elencadas nos Projectos de Lei n.º 217/IX, 240/X e 367/X, bem como na Proposta de Lei n.º 155/IX, designadamente, no âmbito do dever de preservação dos dados por parte dos operadores de comunicação. Também não teve em conta a Directiva n.º 2006/24/CE, de 15 de Março, do Conselho e do Parlamento,

8 Neste sentido, atenda-se aos Pareceres n.os 27/2004, de 8 de Junho, e 29/2004, de 29 de Junho de 2004.

9 *V.g.*, inclua-se, aqui, a questão controvertida referente à *facturação detalhada*.

relativa à "conservação de dados no domínio das comunicações electrónicas" (já publicada no JOUE antes da Reforma de 2007).

e) A Lei n.º 32/2008, de 17 de Julho – a criminalidade grave e os pressupostos estritos

No ano de 2008, o legislador aprovou a Lei n.º 32/2008, de 17 de Julho[10], que transpôs a Directiva n.º 2006/24/CE, que regulou a "conservação e a transmissão dos *dados de tráfego* e de *localização* relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes" (art. 1.º, n.º 1). Ainda assim, o seu regime estabelecia pressupostos mais estritos do que qualquer um dos Projectos Lei *supra* referidos, como a exigência de despacho fundamentado do juiz[11].

Diversamente ao artigo 189.º do CPP de 2007, o artigo 4.º da Lei n.º 32/2008 permite-nos concluir que os dados de base se integram na categoria abstracta dos dados de tráfego[12].

f) A Lei n.º 109/2009, de 15 de Setembro – Lei do Cibercrime

A Lei n.º 109/2009, de 15 de Setembro, aprovou a Lei do Cibercrime (LC), transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a "ataques contra sistemas de informação", adaptando o direito interno à CCiber. Nestes termos, surgem duas inovadoras definições de dados, a saber: os *dados informáticos* (art.º 2.º, al. *b)*) e os *dados de tráfego* (art.º 2.º, al. *c)*)[13]. (realce nosso)

Como se pode observar, a presente lei apresenta um âmbito próprio de regulamentação, ou seja, o da criminalidade informática, bem como o dos regimes cometidos por meio de um sistema informático ou em relação aos quais seja

10 O seu processo legislativo iniciou-se com a Proposta de Lei n.º 161/X, do Conselho de Ministros de 6 de Setembro de 2007.

11 Na redacção do seu art. 3.º, não só dispõe como finalidade exclusiva a "investigação, detecção e repressão de crimes graves", como também impõe que a transmissão de dados só pode ser ordenada ou autorizada por despacho fundamentado do juiz.

12 Prevê que se inserem na categoria de "dados necessários para para encontrar e identificar a fonte de uma comunicação" o " nome e endereço do assinante ou do utilizador registado", assim como o "nome e o endereço de assinate ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação".

13 Cf. Venâncio, 2011: 35.

necessário proceder à recolha de prova em suporte electrónico, tal como não prejudica o regime da Lei n.º 32/2008, de 17 de Julho[14] (arts. 11.º, n.os 1 e 2). Ao contrário desta última, a LC prevê a preservação e acesso a *dados informáticos* e de *tráfego* por ordem do MP, podendo aquela preservação ser também ordenada pelos Órgãos de Polícia Criminal (OPC), perante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora.

Importa realçar que, a preservação dos dados pode ser ordenada por todos os cidadãos (não apenas aos operadores/fornecedores de comunicações) que tenham disponibilidade ou controlo dos *dados informáticos específicos armazenados num sistema informático, incluindo os dados de tráfego*, ficando vinculados ao dever de preservação expedita de dados de modo a *assegurar a confidencialidade da aplicação da medida processual*[15] (art.º 12.º, n.os 1 e 4) e, ainda, ao dever de apresentação dos dados, que implica a comunicação ao processo ou que se permita o acesso ao mesmo, sob pena de punição por desobediência (art. 14.º, n.os 1 e 3), mediante injunção.

O legislador ao prever, no seu artigo 18.º, a intercepção da comunicação electrónica em transmissão, fez referência aos *dados de conte*údo e aos *dados de tráfego*. De acordo com o que será abordado *infra* (ponto 3.), o que se pretendeu foi atender a *dois momentos*: um relativo à *transmiss*ão *das comunicações electr*ónicas, *considerando a tutela constitucional acrescida* do direito da privacidade e da inviolabilidade das comunicações aquando da intercepção em tempo real, *quer quanto aos dados de conteúdo como quanto aos dados relacionados com a comunicação*, sob pena de violação do direito ao segredo das comunicações electrónicas; o outro, relativo à *intromissão em momento posterior* à cessação da comunicação, ou seja, aos dados armazenados, cuja protecção já não se afigura tão rígida por se reportar à protecção da privacidade na sua projecção de *autodeterminação informacional*. Por fim, resta acrescentar que a intercepção só pode ser autorizada pelo juiz, perante requerimento do MP, durante a fase de inquérito e se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter (artigo 18.º, n.º 2 da LC).

14 Cf. Neves, 2011: 237.

15 A par da ordem expedita de dados, enquanto medida com carácter *prévio*, uma outra medida de obtenção de prova com carácter *urgente* pelo perigo de perda irreversível de determinados dados, pode relacionar-se com todos os *dados informáticos* que integram os de *conteúdo* (já não os de comunicação, mas antes informação em forma de dados pessoais).

2.2. As soluções adoptadas no ordenamento jurídico português

a) Considerações gerais

No âmbito do acesso e obtenção de dados relativos às comunicações electrónicas como meios de obtenção de prova baseados na intercepção e registo de comunicações, uma das principais preocupações prendeu-se com a captação do próprio conteúdo da mensagem, sendo que, por vezes, os dados relativos à comunicação afiguram-se mais significativos do que a própria comunicação. Contudo, a "obtenção de dados relativos às comunicações, com vista a fazer prova em processo penal tem que constar expressa e minuciosamente prevista na lei, sob pena de violação do princípio da legalidade"[16], isto porque o direito ao sigilo das comunicações eletrónicas não é um direito absoluto, sucedendo que, ao abrigo do artigo 34.º, n.º 4 *in fine* da Constituição da República Portuguesa (CRP), se prevêm restrições, cabendo à lei ordinária definir os seus limites.

Porém, podia suceder que, numa comunicação electrónica, por não estarem em causa elementos que respeitem ao conteúdo da comunicação, mas perante *elementos externos*, os mesmos eram directamente solicitados aos operadores das comunicações electrónicas, pelos órgãos de polícia criminal (OPC), ou pelo MP, por se considerarem menos lesivos da privacidade da pessoa, já não directamente à inviolabilidade das comunicações, facto que legitimava o acesso por mera solicitação dessas entidades. Diversamente, o acesso aos dados de conteúdo apenas tinha lugar através de um despacho judicial, por se aplicar o regime das escutas telefónicas, precisamente por incidirem sobre o conteúdo da comunicação.

Para além disso, cumpre ter presente que esta necessidade de acesso e de obtenção conflitua com os direitos à reserva da privacidade e à inviolabilidade das comunicações. Gomes Canotiho e Vital Moreira[17] identificam que "o conteúdo do direito ao sigilo da correspondência e dos outros meios de comunicação privada abrange toda a espécie de correspondência de pessoa para pessoa […] e todas as telecomunicações […]. A garantia do sigilo abrange não apenas o conteúdo da correspondência, mas o *tráfego* como tal (espécie, duração, intensidade de utilização)", uma vez que "a Constituição não apenas garante o sigilo da correspondência e dos outros meios de comunicação privados (n.º 1) mas também proíbe toda a ingerência". Seguindo o entendimento de Pedro

16 Cf. Neves, 2011: 209.

17 Cf. Gomes Canotilho & Vital Moreira, 2007: 544 e 545.

Gonçalves[18], os direitos em causa abrangem tanto a proibição do acesso não autorizado de terceiros ao conteúdo das comunicações, a chamada vigilância ou a interceção de comunicações, como a proibição da divulgação e utilização por terceiros desse conteúdo e das circunstâncias (hora, duração, endereços, *et al.*) das comunicações estabelecidas.

b) O contributo dos Pareceres do Conselho Consultivo n.ºs 16/94, de 1996 e 21/2000, de 2000: a divisão tripartida dos dados

Com o intuito de aceder e obter os dados relativos às comunicações electrónicas, a questão inicial relacionava-se com a delimitação dos tipos de dados, dando origem à primeira orientação defendida pela PGR, através dos seus Pareceres do Conselho Consultivo n.ºs 16/94, de 1996 ("TELEPAC, Serviços de Telecomunicações, S.A.") e 21/2000, de 2000[19] ("TMN"). Nos casos que serviram de base a estes pareceres, suscitou-se a questão de saber se as informações e os dados sobre a utilização dos sistemas da rede, requisitados com maior regularidade pela Brigada de Investigação do Crime Informático da PJ, estariam abrangidos pelo sigilo das telecomunicações e, em caso afirmativo, se as informações poderiam ser requisitadas, sem qualquer mandado judicial, directamente pela Polícia Judiciária.

Apesar da complexidade da matéria em causa, adoptou-se uma *distinção tripartida das espécies ou tipologias de dados ou elementos*: os *dados de base* (dados relativos à conexão à rede), os *dados de tráfego* (dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os da rede, por exemplo, localização do utilizador, do destinatário, duração da utilização, data e hora, frequência, entre outros) e, por fim, os *dados de conteúdo* (dados relativos ao conteúdo da comunicação ou da mensagem). Chama-se a atenção para o facto de os *dados de localização* parecem inserir-se entre a categoria dos *dados de tráfego*, embora, *por vezes*, *autonomizados*. (sublinhado nosso)

c) A divisão defendida pela doutrina e pela jurisprudência

Como se pode retirar de algumas decisões proferidas nos tribunais portugueses, a jurisprudência nem sempre foi ao encontro do que se defendeu no

18 Cf. Gonçalves, 1999: 190.

19 Estes Pareceres "Telepac" e "TMN", podem ser consultados, respectivamente, em: http://www.dgsi.pt/pgrp.nsf/0/58101f7b2b6fb7818025689e00501437?OpenDocument e http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8?OpenDocument.

âmbito de uma problemática específica – a sujeição dos diferentes tipos de dados ao sigilo das telecomunicações – que, podendo não se reportar directamente aos tipos de dados relativos às comunicações electrónicas, ajudaram a compreender e a superar as várias dificuldades subjacentes, contribuindo para a sua ponderação *mutatis mutandis*.

Neste sentido, salienta-se o *Acórdão do TC n.º 241/02, de 29 de Maio*[20], que se pronunciou quanto às exigências de obtenção de dados relativos às telecomunicações, considerando que, se os *dados de base* forem disponibilizados pelo titular, em listas públicas de assinantes, os mesmos não estarão abrangidos pelo sigilo das telecomunicações. Já se a lei garante a estes dados um regime de confidencialidade caso o titular opte ou não por os divulgar (reserva da intimidade da vida privada). Com efeito, os dados relativos ao número de telefone, nome e residência do assinante, estariam abrangidos pelo sigilo, tal como resultou do Parecer da PGR de 1996.

Não obstante, no *Acórdão TRL de 23 de Junho de 2004*[21], retrata-se o acesso à *facturação detalhada,* com *trace-back* a localização celular, elaborado com base nos termos dos Pareceres acima referidos e da respectiva legitimidade para a solicitar. Entendeu-se que esta competência cabia, apenas, ao juiz para autorizar o próprio acesso ao conteúdo da conversação telefónica[22]. Por fim, o TRL veio referir que os *dados de base* (*cópia do contrato telefónico*) podem ser solicitados pelo MP, contrariamente aos *dados de tráfego* (a *listagem*), enquanto elementos inerentes à própria comunicação, que exigem que haja prévio despacho judicial.

Uma outra orientação surgiu por parte do *Acórdão TRL de 15 de Maio de 2003*[23], que entendeu, minoritariamente, que a necessidade de despacho judicial só se colocava em matéria de obtenção dos *dados de conteúdo*, sendo que o legislador não quis estender essa supervisão estritamente judicial, aos *dados de base* e aos *dados de tráfego*, podendo estes "ser fornecidos pelos operadores de telecomunicações a solicitação da autoridade judiciária competente para a

20 Consultável em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/ce7999e8a0dc962f802574d4004ef5f9?OpenDocument.

21 Consultável em: http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/033cbd481c837f2180256f620052b6ab?OpenDocument.

22 O MP veio invocar que "a privacidade das comunicações telefónicas ou telemóveis, como corolário da reserva de intimidade da vida privada, [...] a proibição do ulterior acesso de terceiros a elementos que revelem as condições factuais em que decorreu uma comunicação (*factura detalhada*)".

23 Consultável em: http://www.dgsi.pt/jtrl.nsf/0/57573f8a356e0e1580256e91003e8ea2?OpenDocument.

fase de inquérito, ou seja, o Ministério Público". A par desta posição minoritária, o Acórdão do TRL de 27 de Setembro de 2007[24], defendeu que os *dados de tráfego* "não implicam uma devassa como aquela que advém do registo das conversações ou comunicações", julgando com base nesta distinção entre *dados de conteúdo* e *dados de tráfego*, que tinha aplicação no levantamento do segredo profissional, nos termos do art. 135.º do CPP.

Em tese, alguns autores, nomeadamente, Nuno Maurício e Catarina Iria[25], defendem a distinção entre os *dados de conteúdo* e os *dados de tráfego*, considerando que, não obstante, os *dados de tráfego* serem abrangidos pelo sigilo das telecomunicações, sustentam que na tutela destes e dos *dados de conteúdo* estão em causa diferentes bens jurídicos, *i.e.,* nos primeiros, *tutela-se a mera privacidade*, *ao passo que nos segundos, tutela-se a reserva da intimidade*. Esta distinção releva, particularmente, no âmbito da intercepção das comunicações, daí a diferenciação de tratamento da categoria de dados levada a cabo por estes autores, no sentido de se dever conferir uma "menor exigência nos casos de intercepção dos dados de tráfego, atenta a sua menor danosidade a um bem também ele de menor protecção e ainda o seu particular interesse para a investigação da criminalidade mais gravosa". Já para Pedro Verdelho[26], era a divisão tripartida que se afigurava correcta que se devia consagrar.

Ainda assim, contrariamente ao que se contempla no *Acórdão do TRL de 15 de Maio de 2003*, estes autores sustentam que a menor exigência na obtenção dos *dados de tráfego* não se deveria repercutir no afastamento da exclusividade da autorização judicial, antes na consideração da suficiência do *interesse para a descoberta da verdade*, afastando-se o carácter subsidiário do recurso a este tipo de intercepções.

Posteriormente, com a Lei n.º 41/2004, de 18 de Agosto[27], que regula o tratamento de dados pessoais e a protecção da privacidade no sector das comunicações electrónicas, a fundamentação jurisprudencial a exigir despacho judicial para a obtenção de dados de tráfego, para além de se fundar nos Pareceres da PGR, passou, também, directamente a citar a presente lei, nos termos do seu

24 Consultável em: http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/0e870e9e2782243380257839005785c2?OpenDocument.

25 Cfr. Maurício & Iria, 2006: 96-98.

26 Cf. Verdelho, 2004: 126-129.

27 Que veio revogar a Lei n.º 69/98, de 28 de Outubro.

artigo 4.º, n.º 1[28]. Assim, veja-se o *Acórdão do TRG de 10 de Janeiro de 2005*, ao salientar que "a distinção entre dados de tráfego das comunicações e o seu conteúdo é, hoje em dia irrelevante, já que a Lei n.º 41/2004, de 18 de Agosto, equipara os dados de conteúdo para efeitos de garantia da inviolabilidade das comunicações". Isto para concluir que o acesso à *facturação detalhada* exige despacho judicial, ao abrigo do artigo 269.º do CPP, por se tratar de um registo de comunicações[29]. Ao nível da tutela legal, tornou-se, *mutatis mutandis*, anacrónica a equiparação de determinados dados de base aos dados de tráfego. Aliás, exemplo disso é o presente acórdão que se funda na *equiparação dos dados de conteúdo aos dados de tráfego*, com recondução dos dados de base ao âmbito de protecção conferido aos dados de tráfego.

Porém, mais tarde, o *Acórdão do TRE de 26 de Junho de 2007*[30], com fundamento no referido artigo 4.º da Lei n.º 41/2004, de 18 de Agosto, *retoma a divisão tripartida* entre *dados de base*, de *tráfego* e de *conteúdo*, segundo o qual os *dados de base* apenas são necessários ao acesso à rede e instrumentais à comunicação, dispensando-se, assim, a sujeição a despacho judicial para a sua obtenção. Por outro lado, no que concerne aos *dados de tráfego* e aos *dados de conteúdo*, uma vez se tratar de elementos da própria comunicação, estes gozam das garantias de inviolabilidade das comunicações, nos termos do artigo 34.º, n.os 1 e 4 da CRP, do artigo 27.º, n.º 1, al. *g)*, da Lei n.º 5/2004, de 10 de Fevereiro (Lei das Comunicações Electrónicas) e do artigo 4.º da Lei n.º 41/2004, de 18 de Agosto.

Entre outras divergências doutrinais que se colocaram acerca da matéria *sub judice*, estas decisões traduzem, de forma nítida, a seguinte questão: tendo os *dados de base* deixado de ser objecto de discussão do sigilo das telecomunicações, bem como a respectiva legitimidade de autorização a elementos destas, esta situação teria que ver com o facto de poderem ser revelados mediante solicitação de qualquer entidade judiciária ou órgão de polícia criminal, respeitando à conexão à rede e não às comunicações em si, ou por se entender

28 Prevendo que "as empresas que oferecem redes e/ou serviços de comunicações electrónicas devem garantir a inviolabilidade das comunicações e respectivos *dados de tráfego* realizadas através de redes públicas de comunicações e de serviços electrónicos acessíveis ao público".

29 Termos em que "sempre que estiver em causa o fornecimento de dados (sejam eles quais forem) relativo a informações [...], apenas o juiz de instrução pode ordenar o seu fornecimento, verificados que estejam os pressupostos legais".

30 Consultável em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument.

que o nome, a morada e o número de utilizador são elementos que se inserem na categoria mais ampla dos *dados de tráfego*, face aos quais não se pode dispensar, em caso algum, uma autorização judicial? De acordo com isto, Benjamim Silva Rodrigues[31] considera que apenas se identificam os *dados de tráfego* e os *dados de localização*, remetendo a sua definição para o artigo 2.º, n.º 1, als. *b)* e *c)*[32] da Lei n.º 41/2004, de 18 de Agosto. Ademais, o mesmo refere que a inviolabilidade do segredo da mensagem se estende, materialmente, a todos aqueles dados relativos à comunicação, tal como tendo sido este o entendimento do TEDH, segundo o qual a garantia de inviolabilidade das comunicações privadas permanece mesmo depois do termo do processo ou do ciclo informacional e comunicacional, procedendo, nesta medida, a uma extensão temporal.

Em suma, como se tem vindo a analisar, da estruturação tripartida passou-se, agora, para um novo paradigma na ordem jurídica, que assentou numa distinção de *carácter temporal do processo de comunicação*, agrupando em cada uma das fases, todos os dados relativos à comunicação e, por outro lado, posteriores à mesma.

2.3. O novo paradigma na ordem jurídica: a Lei do Cibercrime e a consagração da divisão bipartida

Face ao que se tem vindo a expor, consagrou-se um sustento legal próprio, estabelecendo-se a distinção entre o acesso a *dados armazenados* e o acesso a *dados em transmissão*, ainda que, com diferentes regimes, com base na tutela constitucional do direito da privacidade e da inviolabilidade das comunicações, quer quanto aos dados de conteúdo, como quanto aos dados relacionados com a comunicação. Com efeito, intercepção só pode ser autorizada pelo juiz, perante requerimento do MP, durante a fase de inquérito e se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter – não se bastando com um grande interesse para a descoberta da verdade (art.º 18.º, n.º 2 e 3 da LC, aplicando-se, subsidiariamente o regime do arts. 187.º, 188.º e

31 Cf. Rodrigues, 2008: 459.

32 Reportando-se a "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma" e os dados de localização, "quaisquer dados tratados numa rede de comunicações electrónicas que indicam a posição geográfica do equipamento terminal de um assinante ou de qualquer utilizador de um qualquer utilizador de um serviço de comunicações electrónicas acessível ao público".

190.º do CPP). No que subjaz ao momento posterior à cessação da comunicação, essa protecção já não se afigura tão rígida por se reportar à protecção da privacidade na sua projecção de *autodeterminação informacional*, prevendo-se a autorização ou ordenação pelo juiz, estando em causa um grande interesse para a descoberta da verdade ou da prova[33], ou ainda, os OPC nos casos previstos no art.º 252.º do CPP, aplicando-se por remissão, o regime da correspondência – art.º 179.º do CPP, *ex vi* art.º 17.º da LC.

Esta distinção bipartida com fundamento num reforço de protecção das comunicações vem ultrapassar a distinção tripartida dos dados relativos às comunicações electrónicas, nos exactos termos em que a jurisprudência e a doutrina os conceptualizaram, considerando apenas o *"tipo" do dado e não o "momento" do acesso*[34], isto porque o legislador conferiu uma tutela acrescida ao teor da comunicação privada (protecção da privacidade em face de terceiros). Entende-se que a partir do momento em que a comunicação cumpre o seu destino, cessa a função comunicacional em si, tomando, o destinatário, conhecimento do conteúdo da comunicação, embora não ficando desprotegido, deixa de merecer a tutela constitucional do segredo das comunicações. Isto implica que o conteúdo já encontrado na comunicação "só perde foro de protecção comunicacional, mas não deixa de ser um conteúdo axiológico-normativamente protegido pelo sentido de privacidade contido em qualquer comunicação". Benjamim Silva Rodrigues[35] afirma que, em sede de comunicações electrónicas, estamos perante situações de protecção constitucional ao nível do artigo 35.º da CRP, que consagra o direito à *autodeterminação informacional*, enquanto expressão de protecção daquela privacidade, dada a devassa dos meios informáticos[36], conferindo, assim, um *plus* de protecção a arquivos que já foram comunicação, por aplicação do regime da apreensão da correspondência.

33 O legislador tutelou, de igual forma, o grau de protecção conferido aos meios de obtenção de prova que têm por objecto ficheiros informáticos resultantes do correio electrónico e os que resultam de comunicações postais – situação que não cabe, aqui, analisar.

34 Cf. Neves, 2011: 240.

35 Cf. Rodrigues, 2011: 481.

36 O Tribunal Constitucional Federal alemão previu a possibilidade de dar lugar à aplicação da protecção da integralidade dos sistemas informáticos.

3. A ANÁLISE CRÍTICA DAS OPÇÕES LEGISLATIVAS

3.1. A *descoordenação* legislativa: algumas propostas de resolução

Alguns autores consideraram que esta produção legislativa resultou numa *descoordenação*, aquando das alterações ao CPP, da aprovação das Leis n.os 32/2008, de 17 de Julho, e 109/2009, de 15 de Setembro, suscitando-se dúvidas de interpretação quanto aos âmbitos de aplicação e ao entendimento conceptual em torno dos dados relativos às comunicações electrónicas para efeitos de acesso e obtenção. Nas palavras de Benjamim Silva Rodrigues[37], o legislador português criou uma "difícil encruzilhada interpretativa" e, como afirmou Manuel da Costa Andrade[38], esta "encruzilhada" implicaria modificações que "aconselhavam o legislador português de 2007 a assumir uma mudança de paradigma normativo".

Como sustenta Rita Castanheira Neves[39], tendo-se assistido a várias "contradições – desnecessárias, pensa-se que, […] *o legislador quis prever e regulamentar diferentemente o acesso e obtenção de dados informáticos como pressuposto geral a todos os crimes* ditos informáticos ou que utilizam o computador ou qualquer outro sistema informático para a realização do crime, em grande parte porque a sua prova só é praticamente possível através da recolha de prova em suporte electrónico, consagrando-se aqui requisitos mais flexíveis de admissibilidade".

Para Pedro Verdelho[40], aquando do acolhimento da CCiber, o direito português deveria ter implementado uma "inovação conceptual de grande importância prática, quanto ao que considera *dados informáticos* no âmbito das comunicações"[41], pronunciando-se no sentido da distinção operada entre os *dados de base* e os *dados de conteúdo* (pelo Conselho Consultivo da PGR) ter

37 Cf. Rodrigues, 2011: 518.

38 Cf. Andrade, 2009: 184.

39 Cf. Neves, 2011: 236.

40 Cf. Verdelho, 2004: 126-129.

41 Relativamente ao tráfego das comunicações na *Internet*, cumpria distinguir um grupo de dados (de base e conteúdo) que, embora referentes ao tráfego, não se reconduzem aos dados de tráfego telefónico, os quais dizem respeito à factura detalhada e ao *trace-back*. A informação daí adveniente também não é susceptível de ser reconduzida à categoria dos dados de base, por nada revelarem sobre o titular do acesso à rede, o local onde se encontra ou a sua identidade, nem à categoria dos dados de conteúdo, por não ser relativa ao conteúdo da comunicação, emissor ou receptor. Deste modo, estariam em causa *dados individuais*, reportando-se "a uma singela comunicação e nada revelam quanto a outras eventuais comunicações efectuadas ou recebidas", ou seja, a "dados pertencentes a um terceiro tipo, de natureza intermédia e diferente [...] há que concluir que não poderão ser-lhes extensíveis as reservas aplicáveis aos dados de conteúdo".

de ser "ajustada às realidades do ambiente cibernético". Contudo, considerou que a solução passasse, antes, por duas fases distintas dos dados (*tráfego* ou *conteúdo*) que implicam diferentes pressupostos de acesso. Assim, este autor entendeu que, para determinar o dia em que uma pessoa acedeu à *Internet*, não há necessidade de obter, primeiramente, despacho judicial, uma vez que esta informação nada revela sobre a pessoa investigada ou outras eventuais comunicações que possa ter efectuado, diferentemente da *facturação detalhada*.

Na senda do que veio consagrar a LC, Rita Castanheira Neves salienta que *importa mais olhar ao momento de vida do dado, do que propriamente à sua classificação funcional*, na medida em que, "se uma comunicação electrónica é interceptada, o acesso ao seu conteúdo, bem como aos dados relativos à sua origem, destino, trajecto, hora, data, tamanho, duração e tipo de serviço, tem de ser legislativamente tratado em função da tutela constitucional das comunicações privadas, exigindo, pelo menos, a intervenção do juiz, uma delimitação efectuada por um catálogo de crimes e por um catálogo de pessoas susceptíveis de serem visadas e um rígido critério de indispensabilidade da prova para a descoberta da verdade", mas se se estiver perante o acesso a conteúdos e a dados relacionados que, já se encontram no seu período de armazenamento, apenas se tutela a protecção da privacidade, na vertente de *autodeterminação informacional*. Os *dados de base* não sofreram qualquer variação no regime de acesso, por se tratar de dados de conexão à rede de comunicação e não dados das comunicações entre si, sendo que a protecção que lhes é conferida encontra-se a nível da privacidade e não, eventualmente, da inviolabilidade da comunicação, pelo que só lhes devem aplicar os últimos requisitos. Para os *dados de localização*, deveria diferenciar-se os que dependem de uma comunicação dos que não necessitam de comunicação por assentarem nos próprios aparelhos de comunicação[42].

Seguindo Manuel da Costa Andrade[43], cumpria valorar a posição de domínio do visado pela diligência, no sentido de a mesma exigir que a protecção da inviolabilidade da comunicação se mantenha. Nestes casos, a efectiva tutela jurídica da inviolabilidade das telecomunicações comporta uma *específica situação de perigo* criada no facto da comunicação estar *sujeita ao domínio e à heteronomia de um sistema de telecomunicações*. Assim, quanto aos *dados de conteúdo*, o

42 *V.g.*, os dados produzidos são dados de comunicação no caso de se obter a localização de pessoa, pelo seu telemóvel, unicamente através do início da chamada.

43 Cf. Andrade, 2009: 158.

destinatário dispõe dos meios e das faculdades para auto-tutelar a subsitência dos dados daquela comunicação, contrariamente aos *dados de tráfego*, que não chegam a estar na esfera de domínio do titular dos dados, estando sempre na efectiva disposição dos serviços que usam as redes públicas de comunicação, concluindo que "parece, pois, razoável defender que as buscas que tenham por objecto *dados de tráfego* fiquem sujeitas à necessidade de despacho judicial, já que se tratam de dados que figuram sempre e irremediavelmente ligados ao processo comunicacional […]".

3.2. Posição pessoal

Analisadas as orientações ou opções legislativas e o pensamento que esteve na base da doutrina e da jurisprudência, cabe ponderar e, seguidamente, colocar a *vaexata quaestio*: das supostas inovações…verdade, utopia ou falta de realismo?

Tendo em conta a evolução legislativa, os sucessivos Projectos de Lei n.ºs 217/X, 240/X e 367/X e a Proposta de Lei n.º 155/IX, apesar de contemplarem disposições inovadoras em sede de obtenção de prova digital electrónica na Internet, pouca ou nenhuma expressão tiveram na nossa ordem jurídica, sendo certo que pode ter sido reflexo da instabilidade política que se fazia sentir. Por outro lado, as opções legislativas, designadamente, a Reforma do CPP, bem como a LC, revelaram algumas debilidades. Veja-se: a primeira denotou uma ausência de ponderação em matéria de recolha de prova electrónica, em particular, na diversidade dos dados, além de não ter adaptado o acesso a comunicações escritas por via telemática ao regime da apreensão da correspondência, tutelando na mesma norma, bens jurídicos com distintos âmbitos de protecção constitucional – a verdadeira "oportunidade perdida"[44]; na segunda, o legislador optou por uma via sistemática desintegrada do CPP.

Contrariamente a alguns autores[45], esta autonomização de regime plasmada na LC consagra uma tutela mais eficaz por meio de uma lei extravagante do que por via da inserção sistemática no CPP, para facilitar a tarefa do intérprete e aplicador do Direito. Afinal, a cibercriminalidade[46] reporta-se a uma matéria especial, com disposições materiais penais e processuais penais próprias. A LC

44 Cf. Mesquita, 2010: 88.

45 Cf. Mesquita, 2010: 101 e 102.

46 Cf. Brenner, disponível em http://www.crime-research.org/library/Susan.htm.

foi a "oportunidade de ouro", consubstanciando uma verdadeira "Reforma" no que concerne às disposições processuais e, em particular, permitiu cessar o anacronismo travado pelo jurisprudência e pela doutrina sobre a visão redutora da tripartição ou quadripartição de dados, que andando à deriva conceptual, com o Acórdão do TRG de 10 de Janeiro de 2005, dobrou o Cabo das Tormentas, não fazendo sentido que, tal como entendeu Pedro Verdelho (*supra* referido) e alguma jurisprudência, se reconheça a necessidade de tutelar três categorias de dados com fundamento e autonomia para originar três regimes distintos.

Assim, a querela acerca da tipologia dos dados relativos às comunicações electrónicas, não só se encontra ultrapassada por um sustento legal próprio, que procede, antes, à divisão bipartida – já não do tipo de dados, mas de momentos – consagrando-se um novo paradigma, mas também parece, actualmente, não fazer sentido, visto a própria evolução legislativa não estabelecer qualquer tipo de diferenciação de dados, desde a Lei n.º 41/2004, de 18 de Agosto, que equiparou os dados de conteúdo aos dados de tráfego, para efeitos de garantia da inviolabilidade das comunicações, até então. Parece que o intuito do legislador foi consagrar um regime "desligado" de preocupações conceptuais relativas ao tipo de dados e garantístico dos direitos de protecção da privacidade e da inviolabilidade das comunicações, em simultâneo, para os dois momentos em que opera a transmissão dos dados, resultando dessa bipartição, diferentes regimes jurídicos (veja-se *supra*, cap. I, ponto 3).

Em jeito de conclusão, pensa-se que a tutela do direito à inviolabilidade das comunicações (art. 34.º da CRP) começa onde acaba a conceptualização formal do tipo de dados. Mais do que "definir", urge "tutelar" eficazmente o teor da comunicação na sua globalidade[47], visto existir características comuns entre os vários tipos de dados, basta atender às definições legais previstas pelo legislador. Salvo melhor opinião, o ponto de partida para a resolução do problema colocado não passa pela tentativa de adopção de definições consensuais ou unívocas sobre as categorias de dados para, consequentemente, estabelecer os respectivos regimes ou tão pouco uma convergência por parte da doutrina ou da jurisprudência, passando antes pela sua equiparação, pelo que se deve abandonar aquela tese, nos exactos termos em que o fez a LC.

47 Cf. Moniz, 1997: 231-298.

4. CONCLUSÃO

De acordo com tudo o que se expôs, por um lado, a evolução legislativa denotou algumas debilidades para a ordem jurídica, "ficando áquem das exigências nacionais e internacionais"[48], por outro lado, a doutrina e a jurisprudência tentaram de apresentar soluções que contribuíssem para suprir essas as lacunas legislativas, como se pode verificar *supra*.

No nosso ordenamento jurídico, o legislador consagrou um novo paradigma com a LC (Lei n.º 109/2009, de 15 de Setembro), que permitiu ultrapassar a divisão tipológica (tripartida) dos dados relativos às comunicações electrónicas, para efeitos de acesso e de obtenção, tendo, antes, optado por uma divisão temporal (bipartida) que atende ao momento em que ocorre o acesso, bem como à tutela do direito à inviolabilidade da comunicação e à privacidade, na sua vertente do direito à *autodeterminação informacional* (arts. 34.º e 35.º da CRP), agrupando em cada uma das fases, todos os dados relativos à comunicação e posteriores à mesma.

Como tive oportunidade de salientar na última parte do presente trabalho, o primeiro passo para a solução para o nosso problema passa pela equiparação dos vários tipos de dados, como entendeu o Acórdão do TRG de 10 de Janeiro de 2005, centrada na efectiva garantia da inviolabilidade das comunicações e o segundo passo, dado pela LC, relativamente à separação dos momentos de acesso (*dados armazenados* ou a *dados em transmissão)*, reforçando, assim, em especial, a tutela constitucional do direito da privacidade e da inviolabilidade das comunicações, independentemente do tipo de dados em causa.

48 Cf. Lourenço, 2002: 263-348.

BIBLIOGRAFIA

Andrade, Manuel da Costa

2009 *Bruscamente no Verão Passado – A reforma do Código do Processo Penal, Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra: Coimbra Editora.

Brenner, Susan W.

2016 *"Is There Such a Thing as "Virtual Crime?"*, disponível em http://www.crime-research.org/library/Susan.htm.

Canotilho, José Joaquim Gomes & Moreira, Vital

2007 *Constituição da República Portuguesa Anotada*, 4.ª ed. Revista, Vol. I, Coimbra: Coimbra Editora.

Gonçalves, Pedro

1999 *Direito das Telecomunicações*, Coimbra: Almedina.

Lourenço, Pedro Miguel Januário

2002 "Criminalidade Informática no Ciberespaço 10 anos após a Publicação da Lei n.º 109/91, de 17 de Agosto", in *Instituto Jurídico da Comunicação, Estudos de Direito da Comunicação*, Faculdade de Direito, Universidade de Coimbra.

Madison, Michael J.

2005 "Law as Design: Objects, Concepts, and Digital Things", *Case Western Reserve L. Rev.*, v. 56.

Maurício, Nuno & Iria, Catarina

2006 "As Escutas Telefónicas como Meio de Obtenção de Prova – Necessidade de uma reforma legislativa ou suficiência de uma interpretação conforme?: Ponto de situação numa já *vaexata quaestio*!", *Polícia e Justiça*, III Série, N.º 7, pp.

Moniz, Helena

1997 "Notas sobre a protecção de dados pessoaisperante a informática (O caso especial dos casos pessoais relativos à saúde)", *Revista Portuguesa de Ciência Criminal*, Ano 7.º Fasc. 2, pp.

Mesquita, Paulo Dá

2010 *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Coimbra Editora.

Neves, Rita Castanheira

2001 *As Ingerências nas Comunicações Eletrónicas em Processo Penal – Natureza e respetivo Regime Jurídico do Correio Eletrónico enquanto meio de obtenção de prova*, Coimbra: Coimbra Editora.

Rodrigues, Benjamim Silva
2008 *Das Escutas Telefónicas – A Monitorização dos Fluxos Informacionais e Comunicacionais*, Tomo I, Coimbra: Coimbra Editora.
2011 *Da Prova Penal – Da Prova Electronico-Digital e Criminalidade Informático-Digital*, Tomo IV, 1.ª ed., Lisboa: Rei dos Livros.
Venâncio, Pedro Dias
2011 *Lei do Cibercrime – Anotada e Comentada*, Coimbra: Coimbra Editora.
Verdelho, Pedro
2004 "A obtenção de prova no ambiente digital", *Revista do Ministério Público*, Ano 25, n.º 99, pp. 117-136.

Jurisprudência

TRIBUNAL CONSTITUCIONAL
Acórdão do TC n.º 241/02, de 29 de Maio, Proc. n.º 444/01.
TRIBUNAL DA RELAÇÃO
Acórdão do TRL de 23 de Junho de 2004, Proc.n.º 8950/2003-3.
Acórdão do TRL de 15 de Maio de 2003, Proc. n.º 10011/2003-3.
Acórdão do TRL de 27 de Setembro de 2007, Proc. n.º 3142/09.3PBFUN-A.L1-5.
Acórdão do TRG de 10 de Janeiro de 2005, Proc. N.º 2189/04-1.
Acórdão do TRE de 26 de Junho de 2007, Proc. n.º 581/12.6PLSNT-A.L1-5.