TRIBUNAL DA COMARCA DE VINHAIS

Anúncio n.º 7459/2009

Processo: 577/09.5TBBGC

Insolvência pessoa colectiva (Requerida)
Requerente: Armandino Abílio Cunha Madureira de Almeida
Insolvente: Afonso Urca & Ca, L.da

Publicidade de sentença e citação de credores e outros interessados nos autos de Insolvência acima identificados

No Tribunal Judicial de Vinhais, Secção Única de Vinhais, no dia 17-06-2009, às 09:30 horas, foi proferida sentença de declaração de insolvência do(s) devedor(es):

Afonso Urca & Ca, L.da:, NIF 504641867, Endereço: Lugar de Portela dos Frades, 5320-000 Vinhais, com sede na morada indicada.

São administradores do devedor:

José Joaquim Urça, , Endereço: Rua Portela dos Frades, 20, Vinhais, 5320-325 Vinhais

Adriano Domingos Afonso, Endereço: Portela dos Frades, N.º 20, Vinhais, 5320-000 Vinhais

Maria de Lurdes Gonçalves, Endereço: Portela dos Frades, N.º 20, Vinhais, 5320-000 Vinhais

a quem é fixado domicílio na(s) morada(s) indicada(s).

Para Administrador da Insolvência é nomeada a pessoa adiante identificada, indicando-se o respectivo domicílio.

Dr.ª Daniela Fernandes, domicilio: Praça da Bom Sucesso, 61, Trade Center, 5.º Dala 507 — 4150-146 Porto

Ficam advertidos os devedores do insolvente de que as prestações a que estejam obrigados, deverão ser feitas ao administrador da insolvência e não ao próprio insolvente.

Ficam advertidos os credores do insolvente de que devem comunicar de imediato ao administrador da insolvência a existência de quaisquer garantias reais de que beneficiem.

Declara-se aberto o incidente de qualificação da insolvência com carácter pleno (artigo 188.º e seguintes do CIRE)

Para citação dos credores e demais interessados

correm éditos de 5 dias.

Ficam citados todos os credores e demais interessados de tudo o que antecede e ainda:

O prazo para a reclamação de créditos foi fixado em 30 dias.

O requerimento de reclamação de créditos deve ser apresentado ou remetido por via postal registada ao administrador da insolvência nomeado, para o domicílio constante do presente edital (n.º 2 artigo 128.º do CIRE), acompanhado dos documentos probatórios de que disponham.

Mesmo o credor que tenha o seu crédito por reconhecido por decisão definitiva, não está dispensado de o reclamar no processo de insolvência (n.º 3 do Artigo 128.º do CIRE).

Do requerimento de reclamação de créditos deve constar (n.º 1, artigo 128.º do CIRE):

A proveniência do(s) crédito(s), data de vencimento, montante de capital e de juros;

As condições a que estejam subordinados, tanto suspensivas como resolutivas;

A sua natureza comum, subordinada, privilegiada ou garantida, e, neste último caso, os bens ou direitos objecto da garantia e respectivos dados de identificação registral, se aplicável;

A existência de eventuais garantias pessoais, com identificação dos garantes;

A taxa de juros moratórios aplicável.

É designado o dia 10 de Novembro de 2009, pelas 09:30 horas, para a realização da reunião de assembleia de Aprovação do relatório, podendo fazer-se representar por mandatário com poderes especiais para o efeito.

É facultada a participação de até três elementos da Comissão de Trabalhadores ou, na falta desta, de até três representantes dos trabalhadores por estes designados (n.º 6 do Artigo 72 do CIRE).

Da presente sentença pode ser interposto recurso, no prazo de 15 dias (artigo 42.º do CIRE), e ou deduzidos embargos, no prazo de 5 dias (artigo 40.º e 42 do CIRE).

Com a petição de embargos, devem ser oferecidos todos os meios de prova de que o embargante disponha, ficando obrigado a apresentar as testemunhas arroladas, cujo número não pode exceder os limites previstos no artigo 789.º do Código de Processo Civil (n.º 2 do artigo 25.º do CIRE).

Ficam ainda advertidos que os prazos para recurso, embargos e reclamação de créditos só começam a correr finda a dilação e que esta se conta da publicação do anúncio.

Os prazos são contínuos, não se suspendendo durante as férias judiciais (n.º 1 do artigo 9.º do CIRE).

Terminando o prazo em dia que os tribunais estiverem encerrados, transfere-se o seu termo para o primeiro dia útil seguinte.

Informação

Plano de Insolvência

Pode ser aprovado Plano de Insolvência, com vista ao pagamento dos créditos sobre a insolvência, a liquidação da massa e a sua repartição pelos titulares daqueles créditos e pelo devedor (artigo 192 do CIRE).

Podem apresentar proposta de Plano de Insolvência o administrador da insolvência, o devedor, qualquer pessoa responsável pelas dívidas da insolvência ou qualquer credor ou grupo de credores que representem um quinto do total dos créditos não subordinados reconhecidos na sentença de graduação de créditos ou, na falta desta, na estimativa do Sr. Juiz (artigo 193.º do CIRE).

28 de Setembro de 2009. — A Juíza de Direito, *Júlia Maria Ferreira Jacome.* — O Oficial de Justiça, *Maria Fernanda Gomes de Freitas Luís.*

302358975

MINISTÉRIO PÚBLICO

Procuradoria-Geral da República

Parecer n.º 79/2008

Telecomunicações — Comunicação electrónica — Dados de Tráfego — Dados de conteúdo — Dados de localização — Escuta telefónica — Investigação criminal — Acesso a dados — Dados em suporte electrónico — Dados em suporte papel — Conservação — Eliminação.

Processo n.º 79/2008

1.ª Aos dados de tráfego, dados de localização, registos de comunicações, registos de chamadas interceptadas e informações sobre o nome, morada e número de assinante que não figurem em listas de assinantes, inscritos em suporte de papel, que sejam produto do tratamento de dados constantes de suporte electrónico com a finalidade de serem transmitidos aos órgãos de polícia criminal e autoridades judiciárias, aplica-se o regime de tratamento dos dados pessoais estabelecido pela Lei n.º 67/98, de 26 de Outubro, lei da Protecção de Dados Pessoais.

2.ª Os dados, registos e informações inscritos em suporte de papel e mencionados na conclusão anterior não deverão ser conservados pelas empresas operadoras para além do período necessário para a sua transmissão às entidades referidas;

3.ª Às empresas operadoras de telecomunicações não é exigido qualquer juízo sobre a relevância das vicissitudes do processo penal em curso quanto à pertinência ou necessidade de conservação dos referidos elementos.

Senhor Procurador-Geral da República,

Excelência:

I

1 — A TMN — Telecomunicações Móveis Nacionais, S. A., em comunicação dirigida a Vossa Excelência (1) veio solicitar a emissão de parecer sobre as duas questões que enuncia da seguinte forma:

> «— Qual o período de tempo que deve ser respeitado pela TMN para arquivamento da documentação inerente à satisfação dos pedidos de informação confidencial dos seus clientes, formulados no âmbito de processos judiciais, pelas autoridades judiciárias e órgãos de polícia criminal com competência para o efeito?
>
> — Qual o período de tempo que deve [ser] respeitado pela TMN para arquivamento da documentação inerente à satisfação de ordens judiciais de intercepção?»

A formulação das duas questões acabadas de transcrever é acompanhada de considerações que fornecem o respectivo contexto e dão indicações sobre o sentido e alcance da pretensão. Diz-se na comunicação da empresa, na parte que mais directamente releva:

> «[...] a TMN responde a diversos pedidos formulados pelos órgãos de Polícia Criminal e Autoridades Judiciárias, no âmbito de processos judiciais, pedidos esse que se traduzem na divulgação de dados pessoais e de tráfego pela TMN, em respeito do deu dever de colaboração com a justiça.

Além dos referidos pedidos a TMN procede também à satisfação de ordens judiciais de intercepção de comunicações, cumprindo os exactos termos do expediente ordenado em cada caso concreto.

Das duas actuações referidas — satisfação dos pedidos de informação confidencial e de ordens de intercepção de comunicações — resulta, naturalmente, um conjunto de documentação, em papel, que a TMN tem vindo a arquivar, sem ter instituído qualquer procedimento e prazo para proceder à destruição dessa documentação.

Tal ausência de procedimento e prazo de destruição de documentação prende-se com a inexistência, no ordenamento jurídico português, de qualquer preceito legal que regule o período de tempo durante o qual tais documentos devem manter-se em arquivo.

No entanto, nos termos da alínea *e*) do artigo 5.º da Lei n.º 67/98, de 26 de Outubro os dados pessoais devem ser "conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior".

Ora, sendo certo que a TMN sabe que está obrigada a conservar a informação de dados pessoais e de tráfego apenas pelo período de "tempo necessário", mas sendo certo também que esta empresa desconhece em que estádio processual se encontram os respectivos autos, no âmbito dos quais as informações são solicitadas e as intercepções ordenadas, desconhecendo ainda quando as correspondentes decisões transitam em julgado, a TMN, por si só, não dispõe de qualquer meio que lhe permita conhecer da pertinência e ou da necessidade da guarda da referida documentação em cada situação concreta.»

E acrescenta-se mais à frente a terminar:

«A resposta a estas questões torna-se premente, por forma a que a TMN possa estar certa de que, com a destruição da documentação em causa, não põe em causa eventuais interesses legítimos que devam ser acautelados, mas que não incorra na violação de qualquer obrigação que se lhe imponha, tendo em conta os imperativos constitucionais aplicáveis no âmbito da reserva da intimidade da vida privada e familiar, ao caso, dos clientes da TMN».

Após a elaboração de uma informação jurídica do Gabinete (2), Vossa Excelência, atenta a sensibilidade das questões colocadas, entendeu submeter o assunto à apreciação do Conselho Consultivo.

Cumpre emitir o solicitado parecer, que vem qualificado de urgente.

II

2 — Dos termos da consulta retira-se que a TMN recebe, por escrito segundo nos é dado perceber, solicitações, provenientes de órgãos de polícia criminal e autoridades judiciárias, de fornecimento de «informação confidencial dos seus clientes» relativa a «dados pessoais e de tráfego» e também «ordens judiciais de intercepção de comunicações». Procederá pelos seus serviços e canais internos à pesquisa dos elementos necessários para os efeitos pretendidos. Coligidos estes, remetê-los-á também por escrito, ou seja, em suporte de papel, às entidades que os solicitaram. Termina neste ponto a sua colaboração com a justiça.

No entanto, dando cumprimento a normas e práticas internas de funcionamento, procederá ao arquivamento da documentação em papel gerada pelos pedidos recebidos e pela sua satisfação. O texto da consulta não concretiza nem identifica o conteúdo desse material, mas também será de supor que dele façam parte informações submetidas a algum especial regime de confidencialidade, na medida em que a consulta deixa entender, ao citar a Lei n.º 67/98, lei da Protecção dos Dados Pessoais, a respeito da conservação de dados, que os documentos deverão ter tratamento diferenciado do restante expediente. À empresa afigura-se que o arquivamento não deverá ter uma duração indefinida que impeça a destruição, que se compreende seja do seu interesse, da documentação em causa.

Neste contexto, a análise a que se procederá baseia-se no pressuposto de que a documentação arquivada contém elementos, respeitantes a matéria de telecomunicações, submetidos a regras específicas de protecção e tutela da privacidade de cidadãos cujos dados pessoais, de forma directa ou indirecta, sejam reproduzidos no material arquivado. É este o campo a que se limita o objecto do presente parecer.

3 — O Código Comercial contém um preceito que a uma primeira leitura seria susceptível de ser aplicado à situação descrita. Trata-se do artigo 40.º que, na redacção que lhe foi dada pelo artigo 8.º do Decreto-Lei n.º 76-—A/2006, de 29 de Março, dispõe o seguinte:

«Artigo 40.º

Obrigação de arquivar a correspondência, a escrituração mercantil e os documentos

1 — Todo o comerciante é obrigado a arquivar a correspondência emitida e recebida, a sua escrituração mercantil e os documentos a ela relativos, devendo conservar tudo pelo período de 10 anos.

2 — Os documentos referidos no número anterior podem ser arquivados com recurso a meios electrónicos.»

Na medida em que as sociedades comerciais, conforme o artigo 13.º do Código Comercial, são comerciantes, e sendo a TMN uma sociedade comercial na modalidade de sociedade anónima, a documentação referida na consulta, passados que fossem dez anos de arquivamento (3), poderia ser destruída.

A consulta conduz-nos, porém, a uma área temática dominada por preocupações de protecção e respeito da intimidade da vida privada que são objecto de específica tutela constitucional e de previsão legislativa própria. As questões colocadas não podem, em consequência, ser resolvidas por aplicação das regras a que está submetida a vida empresarial privada em geral.

III

4 — A Constituição consagra no n.º 1 do artigo 26.º o direito de todos à reserva da intimidade da vida privada e familiar e logo no n.º 2 seguinte prescreve que «[a] lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias», para além de consagrar, consequentemente, a inviolabilidade dos meios de comunicação privada, no n.º 1 do artigo 34.º

Em matéria de comunicações electrónicas e no que respeita à tutela da privacidade é aplicável em primeiro lugar o regime da Lei n.º 67/98, de 26 de Outubro, lei da Protecção de Dados Pessoais, que regula a protecção das pessoas singulares no que respeita ao tratamento dos dados pessoais e à livre circulação destes. Pese embora o seu âmbito mais abrangente, esta Lei não é derrogada pela Lei n.º 41/2004, de 18 de Agosto. Com efeito, esta última lei, que se aplica ao tratamento de dados pessoais no contexto das redes e serviços de comunicações electrónicas acessíveis ao público, apenas especifica e complementa as disposições da Lei n.º 67/98 tal como se dispõe no n.º 2 do seu artigo 1.º

É assim que, ainda no âmbito alargado da Lei n.º 67/98, segundo a alínea *a*) do seu artigo 3.º, "dados pessoais" são «qualquer informação de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social». Constitui "tratamento de dados pessoais" «qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição» (alínea *b*) do mesmo artigo). A recolha, conservação e apagamento ou destruição destas informações são consequentemente formas de "tratamento de dados pessoais". Por sua vez, a "interconexão de dados" é uma forma de tratamento que consiste «na possibilidade de relacionamento dos dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade» (alínea *i*) do artigo citado)

O consentimento do titular, de acordo com o artigo 6.º, é regra básica para efeito de admissibilidade do tratamento de dados pessoais, sem prejuízo de situações em que pode ser dispensado ou é pressuposto, como por exemplo, com relevância para o nosso caso, para efeito de execução de contrato ou contratos em que o titular seja parte (alínea *a*) do artigo). Poderá dizer-se que cada pessoa tem direito à sua autodeterminação informacional: caber-lhe-á «escolher e designar quem, quando e como sinais exteriores objectivos daquilo que ela é podem ser ouvidos, registados reproduzidos ou manuseados, questão que ganha especial acuidade nas relações comunicacionais não pessoais» (4).

Por outro lado, «[o]s responsáveis do tratamento de dados pessoais, bem como as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções» (artigo 17.º, n.º 1). No circunstancialismo da consulta acresce a este dever de segredo profissional o segredo de justiça em que, conforme resulta do n.º 8 do artigo 86.º do Código de Processo Penal, estão investidas as pessoas que no âmbito da empresa, por qualquer título, tiverem tomado contacto com o processo penal em curso ou conhecimento de elementos a ele pertencentes, designadamente e desde logo, as pessoas que tiverem manuseado as solicitações recebidas ou tiverem conhecido o respectivo conteúdo.

Para além da imposição de segredo profissional, outra face da protecção da privacidade passa, nos termos do n.º 1 do artigo 14.º da Lei n.º 67/98, pela adopção de «medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados [...]

e contra qualquer outra forma de tratamento ilícito [...]» consignadas no artigo 15.º da Lei n.º 67/98.

5 — A Lei n.º 41/2004 dispõe 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 de comunicações electrónicas acessíveis ao público» (n.º 1 do artigo 4.º). A lei proíbe «a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de intercepção ou vigilância de comunicações e dos respectivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores» (n.º 2 do mesmo artigo 4.º), mas, neste mesmo preceito, admite excepções nos casos previstos na lei. Devem estas ser enquadradas na previsão do n.º 4 do artigo 1.º, que admite, definidas em legislação especial, «as excepções à aplicação da presente lei que se mostrem estritamente necessárias para a protecção de actividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infracções penais».

É definida como "comunicação electrónica" «qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações electrónicas acessível ao público» (alínea *a*) do n.º 1 do artigo 2.º). Nessa comunicação estão envolvidos utilizadores e ou também assinantes. As informações enviadas no âmbito de serviço de difusão ao público em geral, que não possam ser relacionadas com um assinante ou com qualquer utilizador identificável que receba a comunicação não são "comunicações electrónicas" para os efeitos da lei (n.º 2 do artigo 2.º).

Uma comunicação envolve "dados de tráfego". Na definição legal (alínea *d*) do mesmo número e artigo 2.º) "dados de tráfego" são «quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos de facturação da mesma». Mais explicitamente refere o considerando (15) Da Directiva n.º 2002/58/CE, de 12 de Julho de 2002, transposta para o ordenamento jurídico português pela Lei n.º 41/2004, que «[u]ma comunicação pode incluir qualquer informação relativa a nomes, números ou endereços fornecida pelo remetente de uma comunicação ou pelo utilizador de uma ligação para efectuar a comunicação. Os dados de tráfego podem incluir qualquer tradução desta informação pela rede através da qual a comunicação é transmitida, para efeitos de execução da transmissão. Os dados de tráfego podem ser, nomeadamente, relativos ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedidor ou do destinatário, à rede de onde provém ou onde termina a comunicação, ao início, fim ou duração de uma ligação. Podem igualmente consistir no formato em que a comunicação é enviada pela rede».

Do enunciado exemplificativo destes dados constante da lei logo se colhe que neles se compreendem dados pessoais (5). É o seguinte o texto do preceito correspondente:

«Artigo 6.º

Dados de tráfego

[...]

2 — É permitido o tratamento de dados de tráfego necessários à facturação dos assinantes e ao pagamento de interligações, designadamente:

a) Número ou identificação, endereço e tipo de posto do assinante;

b) Número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de início, e duração das chamadas efectuadas ou o volume de dados transmitidos;

c) Data da chamada ou serviço e número chamado;

d) Outras informações relativas a pagamentos, tais como pagamentos adiantados, pagamentos a prestações, cortes de ligação e avisos.

[...]»

A chamada facturação detalhada é um meio colocado ao dispor do assinante para verificar a exactidão dos montantes cobrados pelo prestador do serviço mas, sendo um registo de conversações telefónicas, e, consequentemente, de dados de tráfego, põe em causa a privacidade dos utilizadores das comunicações electrónicas. Certamente por essa razão o artigo 8.º da Lei n.º 41/2004 admite a regulação da matéria com intervenção da Comissão Nacional de Protecção de Dados.

Outra categoria relevante de dados é constituída pelos dados de localização, estreitamente relacionados com os dados de tráfego na medida em que a localização diz respeito ao equipamento terminal de um utilizador do equipamento previamente identificado (6). São dados de localização «quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um assinante ou de qualquer utilizador de um serviço de comunicações electrónicas acessível ao público» na definição da alínea *e*) do n.º 1 do artigo 2.º da Lei n.º 41/2004. Vão aí incluídos a latitude, longitude e altitude do equipamento terminal do utilizador, a direcção de deslocação, o nível de precisão da informação de localização, a identificação da célula de rede em que o equipamento terminal está localizado em determinado momento e a hora de registo da informação de localização, segundo se refere no considerando (14) Da Directiva 2002/58/CE. Estes dados são tratados nas redes móveis digitais para possibilitar a transmissão das comunicações mas tornam praticável a chamada localização celular, através da qual se pode conhecer em que local se encontra o detentor de um telefone móvel e a sua movimentação. Nessa medida são dados pessoais e o regime regra é o de que o respectivo tratamento é apenas permitido se os dados forem tornados anónimos (artigo 7.º, n.º 1 da Lei n.º 41/2004).

É também porque as listas de assinantes contêm dados pessoais que «os assinantes têm o direito de decidir da inclusão dos seus dados pessoais numa lista pública e, em caso afirmativo, decidir quais os dados a incluir, na medida em que esses dados sejam pertinentes para os fins a que se destinam as listas, tal como estipulado pelo fornecedor» (artigo 13.º, n.º 2, da Lei n.º 41/2004, a qual dispõe transitoriamente, no artigo 18.º, que é norma especial, sobre as listas já elaboradas e colocadas no mercado antes da data de entrada em vigor da lei).

6 — Em consonância com o direito à reserva da intimidade e de alguma forma em desenvolvimento deste direito, é afirmada no n.º 1 do artigo 34.º da Constituição a inviolabilidade do domicílio e da correspondência e «dos outros meios de comunicação privada». No n.º 4 deste artigo estabelece-se que «[é] proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal». E quanto a este último ponto é ainda a Constituição, no n.º 8 do artigo 32.º, que estabelece que «[s]ão nulas todas as provas obtidas mediante [...] abusiva intromissão [...] nas telecomunicações». O Código de Processo Penal retoma este comando prescrevendo no n.º 3 do artigo 126.º que, «[r]essalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão [...] nas telecomunicações sem o consentimento do respectivo titular».

Intromissões e ingerências nas telecomunicações só poderão ser acolhidas no nosso ordenamento desde que respeitem o regime das restrições de direitos liberdades e garantias estabelecido nos n.os 2 e 3 do artigo 18.º da Constituição. Sobre esta matéria a Lei n.º 41/2004, conforme já ficou dito, limita-se a admitir as excepções à sua aplicação que se mostrem necessárias «para a prevenção, investigação e repressão de infracções penais», «definidas em lei especial» (artigo 1.º, n.º 4), a qual nesse contexto é o Código de Processo Penal. É assim que o Código, em matéria de prova (Livro III), e quanto aos meios de obtenção da prova (Título III desse Livro), dedica um Capítulo às escutas telefónicas. Neste Capítulo, o artigo 187.º admite a interceptação e a gravação de conversações ou comunicações telefónicas durante o inquérito, autorizadas por despacho do juiz de instrução e mediante requerimento do Ministério Público, relativamente apenas a crimes taxativamente indicados, regime que o artigo 189.º estende à obtenção de outros elementos relevantes neste âmbito.

No texto da consulta diz a TMN que procede à intercepção de comunicações para satisfação de ordens judiciais, omitindo qualquer referência à realização de gravações. Referir-se-á, é de supor, apenas à intercepção em sentido estrito. Trata-se de um procedimento técnico que proporciona o acesso a conversações ou comunicações telefónicas a uma terceira instância onde a comunicação poderá ser escutada e gravada. Essa instância é a Polícia Judiciária, à qual cabe a competência exclusiva para a execução do controlo das comunicações, nos termos do artigo 27.º da Lei n.º 53/2008, de 29 de Agosto, lei de Segurança Interna.

Ao juiz são presentes os elementos recolhidos com base na intercepção, e é também ele que determina a destruição imediata dos suportes técnicos e relatórios manifestamente estranhos ao processo (n.º 6 do artigo 188.º) «ficando todos os intervenientes vinculados ao dever de segredo relativamente às conversações de que tenham tomado conhecimento» (*ibidem*). Durante o inquérito, por sua vez, a requerimento do Ministério Público, o juiz determina «a transcrição e junção aos autos das conversações e comunicações indispensáveis para fundamentar a aplicação de medidas de coacção ou de garantia patrimonial, à excepção do termo de identidade e residência» (n.º 7 do mesmo artigo).

Os suportes técnicos referentes a conversações ou comunicações que não tiverem sido transcritas para servirem como meio de prova «são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo» (n.º 12 do artigo 188.º).

Os suportes técnicos subsistentes após o trânsito, que não tiverem sido destruídos, «são guardados em envelope lacrado, junto ao processo, e só podem ser utilizados em caso de interposição de recurso extraordinário» (n.º 13 do mesmo artigo).

O regime dos dois artigos 187.º e 188.º, designadamente a limitação da sua aplicação na obtenção de prova quanto aos crimes ditos de catálogo enumerados no artigo 187.º e a necessária autorização do juiz de instrução proferida a requerimento do Ministério Público, não é aplicável apenas a conversações ou comunicações telefónicas.

Com efeito, dispõe o n.º 1 do artigo 189.º do Código de Processo Penal que «[o] disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção de comunicações entre presentes».

Por outro lado, «[a] obtenção e junção aos autos de dados sobre a localização celular ou de registo de realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo» (n.º 2 do mesmo artigo 189.º).

O n.º 2 do artigo 189.º do Código de Processo Penal é omisso quanto ao destino dos dados sobre localização celular ou de registos de conversações ou comunicações, trazidos ao processo. É de admitir que, por analogia, lhes seja aplicável o regime do artigo 188.º, já descrito, sobre o material proveniente das gravações quanto à sua junção aos autos, destruição ou conservação em envelope lacrado (7).

Os artigos 187.º, 188.º e 189.º são aqui referidos na redacção que lhes foi dada pela Lei n.º 48/2007, de 29 de Agosto (8). Antes dessa data o Código de Processo Penal limitava-se a prever e regular a intercepção e a gravação de conversações ou comunicações telefónicas ou transmitidas por outro meio técnico, aí se compreendendo designadamente e de forma expressa o correio electrónico. Ficavam de fora diligências respeitantes à obtenção de outro tipo de informações, designadamente sobre identificação e morada dos clientes das operadoras de telecomunicações, dados de tráfego e localização celular. Com a redacção vigente do n.º 2 do artigo 189.º a obtenção de dados sobre a localização celular e de registos de conversações ou comunicações, que são dados de tráfego, só podem ser ordenadas ou autorizadas pelo juiz, em qualquer fase do processo e quanto aos crimes de catálogo (9).

IV

7 — As considerações anteriores mostram as preocupações que o legislador vem justificadamente revelando no que respeita à tutela da privacidade dos dados pessoais dos cidadãos utilizadores de meios electrónicos de comunicação. Para esse efeito instituiu medidas de protecção da confidencialidade de informações que apenas cedem perante os valores preponderantes da investigação das infracções criminais e de punição dos infractores, não por decisão dos órgãos de polícia criminal ou do Ministério Público, mas na sequência de autorização que tem de ser solicitada e obtida do juiz de instrução, no seu estatuto de instância não envolvida de forma directa e imediata no inquérito e nos actos de obtenção da prova praticados nessa fase.

Não surpreende, assim, que preocupações de sentido semelhante acompanhem tudo o que diz respeito à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas. É certo que esses dados, depois da utilização para os fins a que directa e imediatamente se destinam, permanecem sob o signo da confidencialidade e continuam submetidos a segredo profissional. Mas, perdida a sua utilidade inicial e necessária, a sua subsistência viabiliza a sua utilização para outros fins, que podem ser fins ilícitos. É para prevenir situações de utilização ilícita que a lei determina que, como princípio orientador, sejam apagados ou tornados anónimos. Contudo, esta orientação prevalecente teve de contemporizar com valores atendíveis de sentido contrário que justificam a conservação dos dados por tempo limitado. Esses valores são aqueles que resultam da consideração dos imperativos da investigação e punição dos crimes. A este respeito é elucidativa a evolução ocorrida no âmbito do ordenamento comunitário e, na esteira deste, na legislação portuguesa.

8 — Dispunha o diploma que entre nós veio inicialmente regular o tratamento dos dados pessoais e a protecção da privacidade no sector das telecomunicações, a Lei n.º 69/98, de 28 de Outubro, que os dados de tráfego deviam ser apagados ou tornados anónimos após a conclusão da chamada (n.º 1 do artigo 6.º), sem prejuízo da possibilidade de tratamento de dados relativos à facturação dos serviços prestados até final do período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado (n.º 3 do mesmo artigo), ou do seu tratamento com o consentimento do assinante para outras finalidades determinadas (n.º 4) A Lei nesta parte transpunha e acompanhava o conteúdo da Directiva 97/66/CE, de 15 de Dezembro de 1997.

Esta Directiva veio a ser substituída pela Directiva 2002/58/CE, de 17 de Julho de 2002. Nesta mantiveram-se as orientações anteriores mas foi acrescentada a admissibilidade de conservação de dados «durante um período limitado», «para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas» (artigo 15.º, n.º 1).

Foi esta última Directiva 2002/58/CE transposta para o ordenamento português pela Lei n.º 41/2004, de 18 de Agosto, já várias vezes citada no presente Parecer, que veio revogar a Lei n.º 69/98.

A evolução normativa até à presente data conclui-se com a Lei n.º 32/2008, de 17 de Julho, que transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, de 15 de Março de 2006, em cuja elaboração (10) esteve presente a memória dos ataques terroristas ocorridos em Londres em 2005 e foi evocada «a necessidade de aprovar o mais rapidamente possível medidas comuns relativas à conservação de dados de telecomunicações» (considerando (10)).

A Lei n.º 41/2004, aliás tal como a Directiva que transpõe, é um diploma sobre tratamento de dados pessoais e protecção da privacidade que, no contexto da disciplina da segurança e confidencialidade das comunicações, regula o aspecto parcelar do destino final dos dados de tráfego que foram necessários para a transmissão da comunicação. A Lei n.º 32/2008, tem um âmbito mais restrito porque incide em primeira linha sobre o destino e transmissão dos dados de tráfego e de localização, desenvolvendo a disciplina legal anterior e consagrando soluções novas. Sucede que esta lei, embora publicada em 17 de Julho de 2008, ainda não é eficaz. Nos termos do respectivo artigo 18.º, só produzirá efeitos 90 dias após a publicação da portaria, ainda não publicada, a que se refere o n.º 3 do seu artigo 7.º

9 — Porque a matéria da conservação daqueles dados interessa particularmente na procura de resposta a dar às questões colocadas, abordaremos sucessivamente o regime de cada uma das duas leis, começando por aquela que neste momento é plenamente aplicável, que é a Lei n.º 41/2004.

Determina o artigo 6.º desta lei, na parte directamente relevante para o nosso tema, que «os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações electrónicas, devem ser eliminados ou tornados anónimos quando deixem de ser necessários para os efeitos da comunicação» (n.º 1). No entanto, é permitido o tratamento dos dados referidos no n.º 2 do artigo 6.º, já transcrito no ponto 5. deste Parecer, necessários à facturação dos assinantes e ao pagamento das interligações (corpo do n.º 2 do artigo) «até final do período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado» (n.º 3) (11). Qualquer outro tratamento, a que se referem os n.os 4 e 5 do artigo 6.º, para efeitos de comercialização de serviços ou de fornecimento de serviços de valor acrescentado, só é permitido se o assinante tiver dado o seu acordo.

Quanto aos dados de localização processados para além dos dados de tráfego, a regra geral é a de que o seu tratamento é permitido «apenas se os mesmos forem tornados anónimos» (artigo 7.º, n.º 1). As excepções previstas na lei dizem respeito às chamadas de emergência (n.º 2) Ou à prestação de serviços de valor acrescentado (n.º 3).

Para uma mais completa informação, será útil conhecer o que se dispõe sobre conservação dos dados na Lei n.º 32/2008, de 17 de Julho, que não entrou ainda em aplicação.

O diploma, como se disse, tem um objectivo bem delimitado pois propõe-se regular «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» (artigo 1.º, n.º 1). A conservação e a transmissão dos dados têm por «finalidade exclusiva a investigação, detecção e repressão de crimes graves» conforme enfaticamente se proclama no n.º 1 do artigo 3.º Crimes graves são os «crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima» (alínea *g*) do n.º 1 do artigo 2.º).

A inversão da perspectiva e orientação anteriores (12) é bem patente na imposição de conservação de dados «pelo período de um ano a contar da data da conclusão da comunicação» que o artigo 6.º faz recair sobre os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede de telecomunicações. "Dados", na definição da lei, são «os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador» (alínea *a*) do n.º 1 do artigo 2.º). O diploma contém uma descrição precisa e extensa dos dados a conservar, agrupados em categorias, cada uma delas

desdobrada em listagem de subtipos que será dispensável transcrever. São as seguintes as categorias de dados a conservar:

«Artigo 4.º

Categorias de dados a conservar

1 — Os fornecedores de serviços de telecomunicações electrónicas publicamente disponíveis ou de uma rede de comunicações devem conservar as seguintes categorias de dados:

a) Dados necessários para encontrar e identificar a fonte de uma comunicação;
b) Dados necessários para encontrar e identificar o destino de uma comunicação;
c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;
d) Dados necessários para identificar o tipo de comunicação;
e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

[...]»

A conservação destes dados torna possível a sua transmissão imediata, não em papel, mas por comunicação electrónica nos termos do n.º 3 do artigo 7.º, às autoridades competentes, mediante despacho fundamentado do juiz, conforme se escreve na alínea *a*) do n.º 1 do artigo 7.º Autoridades competentes são, nos termos da alínea *f*) do n.º 1 do artigo 2.º, as autoridades judiciárias e as autoridades de polícia criminal das entidades seguintes: Polícia Judiciária; Guarda Nacional Republicana; Polícia de Segurança Pública; Polícia Judiciária Militar; Serviço de Estrangeiros e Fronteiras; e Polícia Marítima.

O regime da transmissão segue de muito perto a formulação dos n.os 1 e 4 do artigo 187.º do Código de Processo Penal. Dispõe-se o seguinte nos n.os 1 a 4 do artigo 9.º desta Lei n.º 32/2008:

«Artigo 9.º

Transmissão dos dados

1 — A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz de instrução, 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 no âmbito da investigação, detecção e repressão de crimes graves.

2 — A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3 — Só pode ser autorizada a transmissão de dados relativos:

a) Ao suspeito ou arguido;
b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou
c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

4 — A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos.

[...]»

Os dados que se encontrem na posse das autoridades competentes, cujo elenco já ficou indicado, bem como aqueles que tenham sido preservados pelos serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de telecomunicações (referidos no n.º 1 do artigo 4.º) Deverão ser destruídos no final do período de conservação, excepto aqueles que tenham sido preservados por ordem do juiz (alínea *e*) do artigo 7.º), da mesma forma que deverão ser destruídos por ordem do juiz aqueles cuja destruição este determinar (alínea *f*) do mesmo artigo). Sobre esta intervenção do juiz dispõe-se o seguinte:

«Artigo 11.º

Destruição dos dados

1 — O juiz determina, oficiosamente ou a requerimento de qualquer interessado, a destruição dos dados na posse das autoridades competentes, bem como dos dados preservados pelas entidades referidas no n.º 1 do artigo 4.º, logo que os mesmos deixem de ser estritamente necessários para os fins a que se destinam.

2 — Considera-se que os dados deixam de ser estritamente necessários para o fim a que se destinam logo que ocorra uma das seguintes circunstâncias:

a) Arquivamento definitivo do processo penal;
b) Absolvição, transitada em julgado;
c) Condenação, transitada em julgado;
d) Prescrição do procedimento penal;
e) Amnistia.»

Como se referiu, a aplicação da Lei n.º 32/2008 está condicionada à publicação de diploma que entretanto ainda não ocorreu. Registem-se as normas da Lei n.º 32/2008 que regulam esta particularidade:

«Artigo 18.º

Produção de efeitos

A presente lei produz efeitos 90 dias após a publicação da portaria a que se refere o n.º 3 do artigo 7.º».

Dispõe o seguinte este último preceito:

«Artigo 7.º

Protecção e segurança dos dados

[...]

3 — A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação electrónica, nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um grau de codificação e protecção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados.

[...]»

V

10 — No precedente Capítulo IV viemos discorrendo sobre a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas à luz do regime ainda em vigor, estabelecido pela Lei n.º 41/2004, e do regime futuro, constante da Lei n.º 32/2008. Importa agora reverter às questões colocadas na consulta e procurar as correspondentes respostas. E para esse efeito haverá que definir com a necessária precisão o regime que deverá ser aplicado à conservação ou eliminação da documentação que a operadora vem arquivando e que, é de supor, ela terá interesse em destruir. É que da descrição dos regimes a que procedemos não fica claro se aqueles documentos deverão ser encarados como expressão directa de comunicações electrónicas, e a esse título submetidos ao regime das duas leis acabadas de indicar, ou como produto acessório ou lateral dessas comunicações e meros sucedâneos de existentes suportes electrónicos, destes podendo ou devendo ser separados e ser objecto de consideração diferenciada, em termos tais que a esses documentos caiba aplicar outro regime.

A vingar o primeiro termo da alternativa, que insere os dados em causa no âmbito da comunicação electrónica, o princípio geral aplicável no quadro da vigente Lei n.º 41/2004 não é o de estabelecer uma permissão; tem antes o sentido contrário de estabelecer um dever ou imposição — os dados, os documentos em papel entendidos como expressão ou manifestação desses dados, «devem» ser eliminados ou tornados anónimos «quando deixem de ser necessários para efeitos da transmissão da comunicação» conforme se dispõe no n.º 1 do artigo 6.º da Lei n.º 41/2004 Mas "podem" manter-se armazenados para determinados efeitos, designadamente facturação, pagamento de interligações e, com o consentimento do assinante ou utilizador, para prestação de determinados serviços, todavia sempre por tempo limitado (n.os 2 a 5 do artigo 6.º da Lei n.º 41/2004). Esgotado este, revive a obrigatoriedade do apagamento ou de anonimato.

Uma vez satisfeita a solicitação de fornecimento de dados, o decurso e vicissitudes do processo, como adiante se referirá, são matéria irrelevante do ponto de vista da operadora de telecomunicações. Esta só tem que cumprir o que se contém na Lei n.º 41/2004 eliminando os dados que tem em seu poder ou tornando-os anónimos, no condicionalismo previsto no artigo 6.º da citada lei.

Quando entrar em vigor a Lei n.º 32/2008 as regras e procedimentos que vêm sendo seguidos em aplicação da Lei n.º 41/2004 sofrerão alterações sensíveis.

Em primeiro lugar, os ficheiros destinados à conservação de dados terão que «estar separados de quaisquer outros ficheiros para outros fins» (n.º 3 do artigo 3.º da Lei n.º 32/2008) E como que ficam em situação de disponibilidade para acesso e transmissão, mas «bloqueados desde o início da sua conservação, só sendo alvo de desbloqueio para efeitos de transmissão [...] às autoridades competentes» (n.º 2 do artigo 7.º). A

nova lei, por outro lado, deixa de admitir a hipótese, menos radical, de tornar os dados anónimos; os dados devem ser destruídos, conforme resulta das alíneas *e*) e *f*) *d*o n.º 1 do artigo 7.º

Essa destruição está, por sua vez, na relativa dependência de vicissitudes processuais. É certo que os dados devem ser destruídos no final do período de conservação; é essa a regra geral (alínea *e*) Citada). Esta porém deixa de se aplicar se antes dessa data o operador tiver recebido ordem do juiz para a sua preservação. Nesse caso os dados preservados pela via indicada só deverão ser destruídos em cumprimento de ordem recebida do juiz (alínea *f*) Citada), emitida nos termos do n.º 1 do artigo 11.º, já transcrito no anterior ponto 9.

11 — Deverá este regime ser aplicado aos dados em suporte de papel que vêm sendo arquivados após a transmissão aos órgãos de polícia criminal e às autoridades judiciárias dos elementos solicitados?

Há que ter em conta que, à partida, é material e juridicamente viável distinguir entre os dados em suporte de papel e os dados em suporte digital. As informações que constam do suporte de papel são informações que, imediatamente antes da sua transposição para esse suporte, existem e continuam existindo em suporte electrónico, foram obtidas por tratamento automatizado com utilização de equipamento apropriado e nesse estado são susceptíveis de tratamento. Tudo quanto exista em suporte de papel, neste contexto, nada tem de originário porque é produto ou reprodução de dados gerados electronicamente.

A Lei n.º 41/2004 regula o armazenamento de informações por utilização das redes de comunicações electrónicas ou o acesso à informação armazenada no equipamento terminal de um assinante ou de qualquer utilizador (artigo 5.º, n.º 1) E impõe, como regra geral, quanto aos dados de tráfego, que sejam eliminados ou tornados anónimos «quando deixem de ser necessários para efeitos da transmissão da comunicação» (n.º 1 do artigo 6.º), ou seja em momento em que esses dados são eliminados ou tornados anónimos no suporte que permitiu a transmissão da comunicação, que é o suporte electrónico.

A Lei n.º 32/2008 pode ser entendida como lei especial em relação à Lei n.º 41/2004, relativamente à qual introduz aditamentos e estabelece derrogações no que respeita à conservação e transmissão para determinadas finalidades de dados gerados ou tratados no contexto das comunicações electrónicas. Mas também é muito claro, quanto a ela, que tem em vista dados em suporte electrónico. Com efeito, o objectivo que legitima a conservação dos dados é precisamente o de facultar a sua transmissão imediata, «mediante despacho do juiz, às autoridades competentes» (alínea *a*) do n.º 1 do artigo 7.º). Essa transmissão far-se-á mediante comunicação electrónica, rodeada das medidas que assegurem a sua inviolabilidade referidas no n.º 3 do mesmo artigo 7.º, sem intervenção portanto de suportes em papel.

Constata-se assim do que antecede que tanto a Lei n.º 41/2004 como a Lei n.º 32/2008 têm em vista informações em suporte electrónico e apura-se, em consequência, que o regime de conservação e armazenamento previsto e regulado pelas Leis n.º 41/2004 e n.º 32/2008 não é aplicável a documentos em papel que contenham ou reproduzam, na terminologia da consulta, "informação confidencial", "informação confidencial dos clientes", "dados pessoais e de tráfego", ou informações sobre comunicações que foram objecto de intercepção, dados estes todos anteriormente gerados e tratados por via electrónica.

Nesta ordem de ideias, e porque se trata de documentos que contêm dados pessoais, forçoso é concluir que lhes será aplicável o regime da Lei n.º 67/98, de 26 de Outubro, lei da Protecção de Dados Pessoais, designadamente no que respeita à sua conservação.

12 — Já foi feita referência, no anterior ponto 4., a aspectos básicos da Lei n.º 67/98. Por ora, deverá ter-se em conta o que se dispõe neste diploma na alínea *e*) do n.º 1 do artigo 5.º:

«Artigo 5.º

Qualidade dos dados

1 — Os dados pessoais devem ser:

[..]

e) Conservados de forma a exprimir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior;

[...].»

A alínea *f*) do n.º 1 do artigo 23.º prescreve que à Comissão Nacional de Protecção de Dados (CNPD) Compete, em especial «[f]ixar o tempo da conservação dos dados pessoais em função da finalidade, podendo emitir directivas para determinados sectores de actividade», mas não se tem notícia de que o tenha feito no que respeita às comunicações electrónicas. Não estamos também perante situação que vise proporcionar a conservação de dados para fins históricos, estatísticos ou científicos, caso em que a Comissão poderá autorizar um período de conservação por período superior ao referido na alínea *e*) do n.º 1 do artigo 5.º

Diz-nos a consulta que da «satisfação dos pedidos de informação confidencial e de ordens de intercepção de comunicações — resulta, naturalmente um conjunto de documentação em papel, que a TMN tem vindo a arquivar». É a este circunstancialismo que teremos de aplicar a regra segundo a qual a conservação dos dados pessoais em suporte de papel é permitida mas apenas por tempo limitado — aquele que, nos termos da alínea *e*) do artigo 5.º da Lei n.º 67/98, for necessário para a prossecução das finalidades de recolha ou de tratamento posterior.

A satisfação dos pedidos e ordens recebidos requer a realização de operações automatizadas com vista à selecção, de entre o fluxo de comunicações electrónicas que utilizam os equipamentos da empresa requerida, dos elementos relevantes para dar resposta à solicitação recebida — registos de chamadas, dados de tráfego, dados de localização, informações sobre assinantes que não sejam acessíveis por consulta de listas públicas, definição das comunicações que devem ser interceptadas e estabelecimento das ligações necessárias para o efeito, entre outros possíveis. Temos aí operações de recolha e tratamento de dados pessoais que serão passadas a suporte de papel e que não têm outra finalidade que não seja a da transmissão dos elementos de informação recolhidos à entidade que os solicitou.

Ora bem, compreende-se que os dados recolhidos possam ou tenham de ser conservados pelo tempo necessário à preparação da sua transmissão (13). Operada esta, cessa a razão de ser da conservação dos dados recolhidos pela entidade solicitada e a documentação em papel poderá ser destruída após a transmissão.

Manter essa documentação na disponibilidade da empresa operadora, inclusivamente e sobretudo na hipótese mais extrema, ou seja, depois de eliminados os dados do originário suporte electrónico ou digital ou tornados anónimos neste último suporte, seria subverter as finalidades que a lei pretende prosseguir e que são as de evitar que os dados em causa possam ser lidos, copiados, alterados ou submetidos a qualquer outro tipo de tratamento por pessoa não autorizada,.

Os dados depois de transmitidos e recebidos pelas entidades destinatárias passam a depender das vicissitudes dos respectivos processos e a estar submetidos a um regime que já descrevemos e que está estabelecido no artigo 188.º do Código de Processo Penal. Nos autos ficará sempre, pelo menos, o expediente e cota da recepção, que comprovarão o cumprimento da solicitação por parte da operadora. Consequentemente, a empresa de telecomunicações não é chamada a formular qualquer juízo sobre a pertinência ou a necessidade de guardar a documentação gerada em resultado do tratamento de dados, necessário para satisfazer a solicitação que recebeu.

Não será despiciendo deixar referido que a eliminação dos suportes de papel poderá não prejudicar o acesso posterior a dados em suporte digital, se tal vier a mostrar-se necessário para suprir qualquer falta, erro ou deficiência na transmissão, desde que os dados em suporte electrónico ainda não tenham sido eliminados ou tornados anónimos por ainda não se ter esgotado o prazo para a sua conservação nesse suporte. O regime aplicável à conservação em suporte de papel de dados pessoais é o regime geral de tratamento dos dados pessoais que, note-se, não se confunde com o regime de tratamento dos dados pessoais utilizados em comunicações electrónicas, que é um regime especial, como se disse. A distinção entre os dois regimes torna-se patente nestas situações em que os suportes em papel deverão ser destruídos, enquanto, tanto por aplicação da Lei n.º 41/2004 como da Lei n.º 32/2008, os dados em causa poderão subsistir em suporte electrónico ou mesmo terão de subsistir, por um ano, por aplicação da Lei n.º 32/2008, quando esta entrar em vigor.

Seja como for, a manutenção em suporte de papel por tempo indefinido não pode garantir em todos os casos a recolha de todos os dados relevantes para a investigação nem a plena satisfação dos pedidos recebidos. Basta pensar na hipótese de os elementos já terem sido eliminados antes de ter sido recebido o pedido, por entretanto ter decorrido o prazo da sua conservação em suporte digital. Nesse caso a satisfação plena das solicitações não será possível.

VI

Em face do exposto, formulam-se as seguintes conclusões:

1.ª Aos dados de tráfego, dados de localização, registos de comunicações, registos de chamadas interceptadas e informações sobre o nome, morada e número de assinante que não figurem em listas de assinantes, inscritos em suporte de papel, que sejam produto do tratamento de dados constantes de suporte electrónico com a finalidade de serem transmitidos aos órgãos de polícia criminal e autoridades judiciárias, aplica-se o regime de tratamento dos dados pessoais estabelecido pela Lei n.º 67/98, de 26 de Outubro, lei da Protecção de Dados Pessoais.

2.ª Os dados, registos e informações inscritos em suporte de papel e mencionados na conclusão anterior não deverão ser conservados pelas empresas operadoras para além do período necessário para a sua transmissão às entidades referidas;

3.ª Às empresas operadoras de telecomunicações não é exigido qualquer juízo sobre a relevância das vicissitudes do processo penal em curso quanto à pertinência ou necessidade de conservação dos referidos elementos.

Este parecer foi votado na Sessão do Conselho Consultivo da Procuradoria-Geral da República, de 7 de Maio de 2009.

Fernando José Matos Pinto Monteiro — José Luís Paquim Pereira Coutinho, relator — *Fernando Bento,* com declaração de voto em anexo — *António Leones Dantas — Maria Manuela Flores Ferreira — José David Pimentel Marcos — Alberto Esteves Remédio — João Manuel da Silva Miguel — Maria de Fátima da Graça Carvalho — Manuel Pereira Augusto de Matos — Fernando Bento* — declaração de voto.

Subscrevo o parecer, nas suas conclusões e fundamentação.

Cumpre, todavia, esclarecer que o preceito decorrente da alínea *e*) do n.º 1 do artigo 5.º da Lei n.º 67/98, de 26 de Outubro, não impõe que a operadora de telecomunicações, logo que expeça uma comunicação escrita dirigida a uma autoridade judiciária informando sobre a efectuação da intercepção de uma linha telefónica para efeitos de escuta ou fornecendo dados de tráfego anteriormente solicitados, proceda, *de imediato*, à destruição de todo o expediente relacionado com esse assunto (ofício recebido a solicitar a intercepção da linha ou os dados de tráfego e respectiva comunicação de resposta, com seus eventuais anexos).

O que esse preceito determina é que os dados sejam conservados durante o «período necessário para as finalidades da recolha ou do tratamento posterior».

Ora, para assegurar as «finalidades da recolha» e o seu «tratamento posterior», não basta garantir que a operadora expediu uma resposta à solicitação da autoridade judiciária. É necessário, também, assegurar, de alguma forma, que essa resposta tenha chegado ao seu destino.

Tendo em conta as circunstâncias específicas do nosso sistema judiciário e as situações, que não são tão raras como isso, de extravio de correspondência (por vezes junta, por erro, a processos a que não diz respeito, sem que tal seja detectado em tempo útil devido à complexidade e ao volume dos mesmos), é essencial, para segurança da própria operadora de telecomunicações, que esta mantenha em arquivo, durante algum tempo, cópia das comunicações que expediu em resposta às solicitações das autoridades judiciárias, para poder comprovar perante estas o cumprimento das suas obrigações legais de colaboração com a justiça em caso de eventual extravio das mesmas.

Deverá tratar-se de um período que permita, em termos de razoabilidade, fazer presumir que a correspondência não terá sofrido extravio, e dentro do qual, a ter-se verificado esse extravio, seria exigível que a autoridade judiciária tivesse interpelado de novo a operadora para satisfazer o pedido anteriormente formulado.

Não competindo a este Conselho, como se assinala no parecer, fixar esse período, parece pertinente a sugestão nele alvitrada de que o mesmo possa ser fixado pela Comissão Nacional de Protecção de Dados, ao abrigo do disposto no artigo 23.º, alínea *f*), da Lei n.º 67/98.

Este parecer foi homologado por despacho do Ministro das Obras Públicas, Transportes e Comunicações, de 18 de Agosto de 2009.

Está conforme.

Lisboa, 25 de Setembro de 2009. — O Secretário da Procuradoria-Geral da República, *Carlos José de Sousa Mendes*.

(1) Ofício de ref.ª ADJCB/101/2007, de 17 de Julho de 2007, entrado na Procuradoria-Geral da República em 20 do mesmo mês.

(2) Informação n.º GI080050.DOC, de 14 de Março de 2008.

(3) Na versão originária do Código Comercial o arquivamento era obrigatório pelo prazo de vinte anos, que veio a ser reduzido para dez anos pelo artigo 1.º do Decreto-Lei n.º 41/72, de 4 de Fevereiro.

A redacção dada pelo Decreto-Lei n.º 76-A/2006 introduziu o n.º 2 do artigo 40.º, no qual passou a ser feita menção expressa à possibilidade de arquivamento electrónico, e aditou ao n.º 1 do artigo, no qual se referia apenas a correspondência «recebida» pelo comerciante, a referência à correspondência por ele «emitida».

Em caso de liquidação de uma sociedade comercial os documentos da sociedade devem ser conservados por um prazo de cinco anos pelo depositário nomeado pelos sócios (n.º 4 do artigo 157.º do Código das Sociedades Comerciais).

(4) Cfr. Pedro Ferreira, *A protecção de dados pessoais na sociedade de comunicação. Dados de tráfego, dados de localização e testemunhos de ligação*, O Espírito das Leis, Lisboa, 2006, pág. 145-146.

(5) Em pareceres anteriores do Conselho Consultivo (v. o Parecer n.º 21/2000, de 16 de Junho de 2000, homologado e publicado no *Diário da República* n.º 198, II Série, de 28 de Agosto de 2000, que originou a Directiva n.º 5/2000 – Despacho de 7 de Agosto de 2000, o Parecer n.º 16/94-Complementar, de 2 de Maio de 1994, publicado em Pareceres, edição da Procuradoria-Geral da República, vol. VI, pág. 535 e segs., e ainda o Parecer n.º 16/94, de 24 de Junho de 1994, que originou a Circular.n.º 13/94, da Procuradoria-Geral da República) estabelecia-se uma distinção entre três categorias de dados: dados de base, dados de tráfego e dados de conteúdo. Nesta tipologia, os dados de base são os dados necessários à conexão à rede, por exemplo, a identificação do utilizador e a morada bem como o número de acesso, inerentes a uma fase prévia à comunicação, e os dados de tráfego são inerentes à própria comunicação, compreendendo elementos que a esta são necessários e nela intervêm, por exemplo, a direcção, o destino e o trajecto.

Para os efeitos da Lei n.º 41/2004, os dados de base não são autonomizados e surgem imbricados no conceito de dados de tráfego, como se pode perceber da alínea a) do artigo 6.º, que agora se transcreve.

(6) Tenha-se presente o que vem dito no considerando (35) da Directiva 2002/58/CE: «[n]as redes móveis digitais, os dados de localização que fornecem a posição geográfica do equipamento terminal do seu utilizador móvel são tratados para permitir a transmissão das comunicações. Esses dados são dados de tráfego, abrangidos pelo artigo 6.º da presente directiva […]». O referido artigo 6.º da Directiva encontra-se transposto no artigo 6.º da Lei n.º 41/2004.

(7) Neste sentido, v. Paulo Pinto de Albuquerque, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2.ª edição, Universidade Católica Editora, Lisboa, 2008, pág. 528.

(8) Sobre a revisão do Código de Processo Penal operada pela Lei n.º 41/2007, e quanto às matérias que vimos tratando, v. Pedro Verdelho, "A reforma penal portuguesa e o cibercrime", *Revista do Ministério Público*, ano 27, n.º 108, Outubro — Dezembro de 2006, pág. 97 e segs., e, do mesmo Autor, "Técnica no novo C.P.P.: exames, perícias e prova digital", *Revista do CEJ*, n.º 9 (especial), 1.º semestre de 2008, pág. 145 e segs.

(9) Sobre estes aspectos pronunciou-se o Conselho Consultivo antes da entrada em vigor da revisão de 2007 nos Pareceres citados em nota anterior.

Designadamente no parecer de data mais próxima, Parecer n.º 21/2000, entendeu-se que os dados de tráfego só poderiam ser fornecidos pelos operadores de telecomunicações nos termos aplicáveis à intercepção de comunicações.

Também se tomou posição sobre os "dados de base", entendidos como os elementos necessários para acesso à rede pelos utilizadores, compreendendo a identificação e morada destes, e que, para efeitos do contrato de ligação à rede, são por estes fornecidos à empresa operadora a qual por sua vez atribui aos utilizadores o número de acesso. Reconheceu-se que estes dados se encontram cobertos pela regra da confidencialidade, nesse caso de génese privatística ou contratual, a qual «releva de um simples interesse pessoal do utilizador que não contende com a sua esfera pessoal íntima» e entendeu-se nessa conformidade que «poderão ser comunicados, a pedido de qualquer autoridade judiciária, para fins de instrução criminal, em ordem ao prevalecente dever da colaboração com a administração da justiça» (conclusão 3.ª). Em sentido contrário, no Parecer n.º 16/94 tinha sido entendido que estariam submetidos às mesmas garantias que os elementos da comunicação propriamente dita e dessa forma abrangidos pelo regime do artigo 269.º do Código de Processo Penal.

(10) Sobre os antecedentes desta Directiva e para uma perspectiva crítica sobre as opções nela adoptadas v. Pedro Ferreira, "A retenção de dados pessoais nas comunicações electrónicas", em *Estudos comemorativos dos 10 anos da Faculdade de Direito da Universidade Nova de Lisboa*, vol. II, Almedina, Coimbra, 2008, pág. 417 e segs.

(11) Segundo o artigo 10.º da Lei n.º 23/96, de 26 de Julho, na redacção que lhe foi dada pela Lei n.º 12/2008, de 26 de Fevereiro, sobre a protecção do utente de serviços essenciais, nos quais se inclui o serviço de comunicações electrónicas (alínea *d)* do n.º 2 do artigo 1.º, na redacção dada pela Lei n.º 12/2008, citada), o direito ao recebimento do preço do serviço prestado prescreve no prazo de seis meses após a sua prestação.

(12) A inversão opera-se, é bom advertir, em quadro delimitador bem definido. Designadamente, a Lei procede a uma enunciação dos crimes graves em grau de tipificação mais exigente do que aquele que, embora com diferente campo de aplicação, consta do artigo 187.º do Código de Processo Penal. Neste preceito, para além de se referirem tipos criminais concretizados, é admitida a intercepção e gravação de conversações ou comunicações quanto a crimes «[…] puníveis com pena de prisão superior, no seu máximo, a três anos», (alínea *a)* do n.º 1).

(13) Como ficou referido, quando vier a ser aplicada a Lei n.º 32/2008 a transmissão passará a processar-se por via de comunicação electrónica, com aplicação de processos de codificação e protecção (segundo o n.º 3 do artigo 7.º). A intenção é certamente a de obviar ao armazenamento em papel e aos riscos a ele inerentes de quebra de inviolabilidade e confidencialidade.

202356869