ACÓRDÃO N.º 420/2017

Processo n.º 917/16

1.ª Secção

Relator: Conselheira Maria de Fátima Mata-Mouros

Acordam na 1.ª Secção do Tribunal Constitucional

I. Relatório

1. Por despacho de 19 de outubro de 2016 da 1.ª Secção de Instrução Criminal da Instância Central da Comarca de Lisboa foi indeferido o pedido do Ministério Público de autorização de transmissão dos dados de identificação de um utilizador a quem estava atribuído um determinado endereço de protocolo IP.

O pedido tinha sido formulado ao abrigo «das disposições conjugadas dos artigos 176.º do Código Penal, 2.º, alínea g), da Lei n.º 32/2008, de 17 de julho, por referência ao artigo 1.º, alínea j) do Código de Processo Penal (CPP), 4.º e 9.º da citada Lei n.º 32/2008» (cfr. fls. 47, por remissão do despacho de 17 de outubro de 2016, fls. 61). O utilizador em causa era suspeito no processo que tem por objeto a investigação de factos suscetíveis de integrar a prática de crime de pornografia de menores, previsto e punido no artigo 176.º, n.º 1, alíneas *b)*, *c)* e *d)*, do Código Penal, com pena de prisão de um a cinco anos.

O despacho fundamentou o indeferimento na inconstitucionalidade do artigo 6.º da Lei n.º 32/2008, por referência ao artigo 4.º da mesma lei, determinando:

«Em face do exposto:

a) Recuso a aplicação do disposto no art. 6.º da Lei n.º 32/2008 (por referência ao art. 4.º da mesma Lei) por contrariedade aos arts. 18.º e 34.º, n.º 4, da Constituição da República Portuguesa;

b) Apenas por tal motivo, por decorrência do disposto no art. 32.º, n.º 8, da Constituição, indefiro o promovido a fls. 32.»

2. O Ministério Público interpôs recurso desta decisão para o Tribunal Constitucional, ao abrigo do artigo 70.º, n.º 1, alínea *a)*, da Lei da Organização, Funcionamento e Processo do Tribunal Constitucional (Lei n.º 28/82, de 15 de novembro [doravante designada por LTC]), que foi admitido pelo tribunal recorrido.

Os autos prosseguiram para alegações, tendo o Ministério Público sustentado, em conclusão, o seguinte:

« III

Conclusões

1ª. O presente recurso obrigatório do Ministério Público, nos termos do respetivo requerimento de interposição, tem por objeto o despacho do Exmo. Juiz de Instrução, de 19 de Outubro de 2016, «*na parte em que recusou aplicar o disposto no artigo 6º da Lei 32/2008, por referência ao artigo 4º da mesma Lei, com fundamento na sua inconstitucionalidade, por entender que a mesma viola os princípios constitucionais de inviolabilidade do domicílio e da correspondência, artigos 18º e 34º, nº 4 da Constituição da República Portuguesa, na medida em que a obtenção de tais elementos probatórios, por constituir abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, se torna nula*».

2ª. Condicionada ao objeto do processo (e do pedido do Ministério Público nele formulado), a apreciação da inconstitucionalidade da norma contida no art. 6º da Lei 32/2008, por referência ao art. 4º da mesma lei, tal como foi mediatizada pela decisão recorrida para a dirimição do caso concreto, há de restritivamente ser (i) precisada por referência ao art. 4º, nºs. 1, alín. a), 2ª parte e 2, alín. b) - iii), da mesma lei e (ii) subordinadamente conjugada com o art. 9º, igualmente da mesma lei (e não pronúncia sobre a amplitude do sistema de conservação de dados – do sistema em geral e do conjunto de dados globalmente considerados – exorbitantemente desconexionada do quadro da concreta situação dos autos).

3ª. É sujeita a esta dupla restrição na sua dimensão normativa – art. 6º, com referência, mais precisamente, aos nºs. 1, 2ª parte e 2, alín. b) - iii) do art. 4º e subordinadamente conjugado com o art. 9º, todos da Lei 32/2008 –, que o objeto inicial do recurso é delimitado (art. 635º, nº 4 do CPC).

4ª. O presente recurso mostra-se instrumentalmente útil – foi processualmente determinada a preservação dos dados em causa, até 1 de outubro próximo (doc. junto).

5ª. A Lei 32/2008, de 17 de julho, transpõe para a ordem jurídica interna a Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

6ª. O Tribunal de Justiça (TJ), por Acórdão da Grande Secção, de 8 de abril de 2014, proferido sobre dois pedidos de decisão prejudicial (art. 267º do TFUE), apresentados pela Irlanda e Áustria, declarou a invalidade da citada diretiva.

7ª. O juízo de inconstitucionalidade constante da decisão recorrida é emitido na esteira do citado Acórdão, essencialmente para ele remetendo na sua fundamentação.

8ª. A transposição da Diretiva 2006/24/CE pela Lei 32/2008 inscreve-se na evolução verificada no direito comunitário e no direito ordinário interno em matéria de telecomunicações e de prova digital.

9ª. A finalizar a apontada evolução legislativa, a Lei 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

10ª. É precisamente ao abrigo da Lei 109/2009 que, em 9 de Setembro de 2016, é proferido primeiro despacho do Juiz de Instrução a determinar à operadora que comunique ao processo os dados pretendidos pelo Ministério Público.

11ª. A Diretiva 2006/24, com a instituição de um instrumento jurídico comunitário de imposição de conservação de dados, culmina um acidentado e complexo processo em termos de balanceamento entre os polos de liberdade e segurança e vem geneticamente marcada pela sua *dualidade funcional* (nºs. 5 a 6.5 do corpo da alegação).

12ª. Os questionamentos que antecederam a entrada em vigor da Diretiva 2006/24/CE, mantiveram-se ou intensificaram-se para além dessa data, tendo designadamente originado decisões em matéria de constitucionalidade por parte dos tribunais de alguns Estados-membros.

13ª. A validação da diretiva, nos termos do Acórdão do TJ, de 8 de abril de 2014, vem a falhar no teste da observância do princípio da proporcionalidade – em um dos seus segmentos, o da *estrita necessidade.*

14ª. É à luz do princípio da proporcionalidade, no apontado segmento, que, no nº 65 do Acórdão, se afirma *«que a Diretiva 2006/24 não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta. Impõe-se pois concluir que esta diretiva comporta uma ingerência nestes direitos fundamentais, de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário»* (nºs. 7 a 7.3 do corpo da alegação).

15ª. À lei 32/2008, que transpôs a diretiva em causa, se referiu já o Ac. 403/15, no sentido de que *«estabelece amplas garantias no que toca ao acesso e conservação dos dados de tráfego e de localização das comunicações para fins de investigação, deteção e repressão de crimes graves por parte das autoridades».*

16ª. Considerada a jurisprudência constitucional na matéria (nºs. 8.1 a 8.2.2. do corpo da alegação), interessa acentuar que, no caso dos autos, a pretensão do Ministério Público, obviamente não se reportando a *dados de conteúdo*, não visa a obtenção de *dados de tráfego ou de localização.*

17ª. Na verdade, os dados de tráfego e localização, com referenciação do endereço do protocolo IP, constavam do processo. Pretendia-se, tão só, com referência a dados já processualmente adquiridos, a obtenção de *dados de base*.

18ª. Dados *prévios* à própria comunicação e relativos à conexão à rede, «*dados conexos necessários para identificar o assinante ou o utilizador registado*» (art. 1º, nº 1 da Lei 32/2008) – no quadro da citada Lei 109/2009, «*informação diferente dos dados relativos ao tráfego ou ao conteúdo … detida pelo fornecedor dos serviços*» (art. 14º, nº 4), no caso, «*que permita determinar … a identidade, a morada postal … do assinante*» [alín. b) do mesmo número].

19ª. Em suma: visa-se no presente processo a obtenção de dados que *«não assumem a dignidade que lhes permita conferir a proteção constitucional do sigilo das comunicações»*.

20ª. Os dados em causa não são, por outro lado, alcançados por um hipotético juízo de inconstitucionalidade, à luz do princípio da proporcionalidade (conjugadamente, arts. 18º e 34º, nº 4 da Constituição), que devesse ter por objeto a questão da indiscriminada amplitude e duração de conservação, bem como do universo de sujeitos abrangido, sistema que, na transposição da diretiva, se manteve nos arts. 4º e 6º da Lei 32/2008.

21ª. Ao invés da previsão abstrata e hipoteticamente configurada, os dados concretamente pretendidos visam a identificação de determinado *suspeito* em processo criminal [art. 1º, alín. e) do CPP] – e não aleatoriamente referidos a uma qualquer entre *«todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que, no entanto, (…) se encontrem, ainda que indiretamente, numa situação suscetível de dar lugar a ações penais»* (nº 48 do Ac. do TJ, de 8 de abril de 2014, cit.).

22ª. Resta observar, em vista de invocada violação do art. 32º, nº 8 da Constituição, que os dados visados não virão processualmente consubstanciar, a essa luz (independentemente de sujeição a regime de arguição), *prova nula*, desde logo não tendo sido obtida com ofensa à integridade pessoal, a sua conservação e ulterior transmissão, no concreto caso dos autos, nos termos do art. 9º da Lei 32/2008, não poderão ser reconduzidos a situação de *abusiva intromissão* na comunicação.

Termos em que se conclui pela não inconstitucionalidade do art. 6º, com referência aos nºs. 1, 2ª parte e 2, alín. b) - iii) do art. 4º e subordinadamente conjugado com o art. 9º, todos da Lei 32/2008, devendo, em consequência, conceder-se provimento ao recurso e ordenar-se a reforma da decisão recorrida em conformidade com o decidido quanto à questão de constitucionalidade.».

Cumpre apreciar e decidir.

II. Fundamentação

a) Delimitação da norma objeto do processo

3. O presente recurso vem interposto ao abrigo da alínea *a),* do n.º 1, do artigo 70.º da LTC, segundo a qual cabe recurso para o Tribunal Constitucional das decisões dos tribunais que recusem a aplicação de qualquer norma, com fundamento em inconstitucionalidade.

No caso dos autos, o tribunal *a quo* recusou a aplicação «do disposto no artigo 6.º da Lei n.º 32/2008 (por referência ao artigo 4.º da mesma Lei) por contrariedade aos artigos 18.º e 34.º, n.º 4, da Constituição» (cfr. a decisão do despacho de 19 de outubro de 2016, fls. 45).

É o seguinte o teor do artigo 6.º da Lei n.º 32/2008, de 17 de julho:

«As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação.»

4. O preceito remete, assim, para o artigo 4.º da Lei n.º 32/2008, de 17 de julho, que identifica os dados que devem ser conservados (os necessários para «encontrar e identificar a fonte de uma comunicação»; «encontrar e identificar o destino de uma comunicação»; «identificar a data, a hora e a duração de uma comunicação»; «identificar o tipo de comunicação»; «identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento»; e «identificar a localização do equipamento de comunicação móvel») e as entidades que ficam obrigadas à sua conservação (os «fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações»). Ora, deste conjunto de preceitos apenas uma dimensão normativa estava em causa no presente processo, sendo desaplicada pelo juiz *a quo*, nos termos do artigo 204.º da Constituição.

Estando em causa um pedido de acesso a dados de identificação de um utilizador a quem estava atribuído um determinado endereço de protocolo IP, apenas está em apreciação a dimensão normativa relativa ao dever de conservação dos dados necessários para «identificar a fonte de uma comunicação», mais especificamente «no que diz respeito ao acesso à Internet (…)», ao «nome e o endereço do assinante 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» (cfr. artigo 4.º, n.º 1, alínea *a)*, 2.ª parte, e n.º 2, alínea *b)*, subalínea *iii)*, da Lei n.º 32/2008).

A norma desaplicada corresponde ao dever de os «fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações» conservarem «pelo período de um ano a contar da data da conclusão da comunicação», os dados relativos ao «nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP» estava atribuído «no momento da comunicação».

b) Enquadramento da questão de constitucionalidade

b.1. Classificação do tipo de dados em causa

5. O objeto do presente recurso está relacionado com os designados «'metadados', usualmente definidos como 'dados sobre dados', por dizerem respeito a circunstâncias das comunicações, e não ao próprio conteúdo da comunicação» (Acórdão n.º 403/2015, ponto 9).

Sobre esta matéria o Tribunal Constitucional já teve oportunidade de se debruçar, no Acórdão n.º 403/2015, esclarecendo, no seu ponto 9:

«Numa concreta comunicação é possível separar do núcleo duro da informação fornecida ou transmitida um conjunto de marcos ou pontos de referência que lhe dão o respetivo suporte e que permitem circunscrever a informação sob todas as formas. Tais dados são 'informações' que acrescem aos dados e que têm como objetivo informar sobre eles, em princípio, para tornar mais fácil a sua organização. Sendo dados sobre dados ('informação sobre informação'), acabam por fornecer informação sobre a localização, tempo, tipo de conteúdo, origem e destino, entre outras, dos atos comunicacionais efetuados através de telecomunicações ou por outros meios de comunicação.

Como categoria que tem por fim um efeito jurídico é de usar a designação 'dados de tráfego' (…) porque no nosso ordenamento jurídico já há uma definição legal desse enunciado. Com efeito, o artigo 2.º, n.º 1, alínea d), da Lei n.º 41/2004, de 18 de agosto, sobre Segurança nas Telecomunicações, define 'dados de tráfego' como 'quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma'.

A este propósito, o Tribunal Constitucional acolheu, desde o Acórdão n.º 241/2002, de 29/05/2002, uma classificação tripartida (louvando-se, então, nos Pareceres do Conselho Consultivo da Procuradoria-Geral da República n.º 16/94, votado em 24/06/94, na base de dados da DGSI, n.º 16/94 – complementar, votado em 2/05/1996, in Pareceres, vol. VI, págs. 535 a 573, e n.º 21/2000, de 16/06/2000, no Diário da República – II Série, de 28/08/2000) dos dados resultantes do serviço de telecomunicações. Ali se distinguiram:

'(…) os dados relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo'.

Tal classificação tripartida foi retomada pelo Tribunal – assinalando que se mantinha, então, 'consensual' – no Acórdão n.º 486/2009».

Efetivamente, no Acórdão n.º 486/2009, ponto 2.2, o Tribunal Constitucional referiu que:

«Não obstante a evolução legislativa acabada de enunciar, a verdade é que, relativamente ao tipo de dados envolvidos no serviço de telecomunicações, continua a ser consensual, no seio da doutrina e jurisprudência nacionais, a classificação adotada pelo Conselho Consultivo da Procuradoria-Geral da República, que distingue entre dados de base, dados de tráfego e dados de conteúdo (Vide Parecer n.º 16/94/complementar, acessível em *www.dgsi.pt*, e Parecer n.º 21/2000, no DR II Série, de 23 de julho de 2002).

Assim, de harmonia com esses pareceres, no serviço de telecomunicações podem distinguir-se as seguintes espécies de dados:

'Nos serviços de telecomunicações podem distinguir-se, fundamentalmente, três espécies ou tipologias de dados ou elementos: os dados relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; e os dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo.

Sendo os vários serviços de telecomunicações utilizados para a transmissão de comunicações verbais ou de outro tipo (mensagens escritas, dados por pacotes), os elementos inerentes à comunicação podem, por outro lado, estruturar-se numa composição sequencial em quatro tempos: a fase prévia à comunicação, o estabelecimento da comunicação, a fase da comunicação propriamente dita e a fase posterior à comunicação.

No primeiro tempo relevam essencialmente os dados de base, enquanto que nos restantes importa essencialmente a consideração dos dados de tráfego e de conteúdo.

Os dados de base constituem, na perspetiva dos utilizadores, os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço: interessa aqui essencialmente o número e os dados através dos quais o utilizador tem acesso ao serviço.

(…)

Diversamente dos elementos de base (elementos necessários ao estabelecimento de uma base para comunicação), que estão aquém, antes, são prévios e instrumentos de qualquer comunicação, os chamados elementos de tráfego (elementos funcionais da comunicação), como os elementos ditos de conteúdo, têm já a ver diretamente com a comunicação, quer sobre a respetiva identificabilidade, quer relativamente ao conteúdo propriamente dito da mensagem ou da comunicação.

Os elementos ou dados funcionais (de tráfego), necessários ou produzidos pelo estabelecimento da ligação da qual uma comunicação concreta, com determinado conteúdo, é operada ou transmitida, são a direção, o destino (adressage) e a via, o trajeto (routage).

(…)

Estes elementos funcionalmente necessários ao estabelecimento e à direção da comunicação identificam, ou permitem identificar a comunicação: quando conservados, possibilitam a identificação das comunicações entre o eminente e o destinatário, a data, o tempo, e a frequência das ligações efetuadas.

Constituem, pois, elementos já inerentes à própria comunicação, na medida em que permitem identificar, em tempo real ou a posteriori, os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação, devem participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações.

Finalmente, os elementos de conteúdo — dados relativos ao próprio conteúdo da mensagem, da correspondência enviada através da utilização da rede'.»

Na síntese do Acórdão n.º 403/2015, no seu ponto 9, os dados de tráfego dizem respeito «'aos próprios elementos funcionais da comunicação, reportando-se à direção, destino, via e trajeto de uma determinada mensagem' (…), identificam ou permitem identificar a comunicação e, uma vez conservados, possibilitam a identificação das comunicações entre emitente e destinatário, a data, o tempo e a frequência das ligações efetuadas». Por seu turno, dados de localização «consistem em dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de telecomunicações, podendo incidir sobre a latitude, longitude ou altitude do equipamento, sobre a direção da deslocação, sobre a identificação da célula de rede em que o equipamento está localizado em determinado momento e sobre a hora de registo da informação de localização. (…) [T]em-se considerado que os mesmos estão também incluídos no conceito mais amplo de 'dados de tráfego' (assim, Catarina Sarmento e Castro, Direito da Informática, Privacidade e Dados Pessoais, Almedina, 2005, pág. 181). E é nesse sentido que a Lei n.º 32/2008, de 17 de julho, que regula a conservação e transmissão dos dados de tráfego e de localização, reserva a mesma disciplina jurídica para ambos.»

6. A norma em causa, no presente processo, diz respeito à necessidade de os fornecedores de serviços de comunicações eletrónicas conservarem, durante um período de tempo, os dados relativos ao «nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP» estava atribuído «no momento da comunicação». Atendendo ao enquadramento descrito, a questão de inconstitucionalidade a analisar diz respeito a apenas um dos referidos tipos de "metadados": os dados de base. Assim é, pois trata-se de «os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço: interessa aqui essencialmente o número e os dados através dos quais o utilizador tem acesso ao serviço» (cfr. Acórdão n.º 486/2009, ponto 2.2).

b.2. Enquadramento normativo aplicável

7. Quanto ao enquadramento normativo aplicável no âmbito dos "metadados", podemos socorrer-nos novamente do Acórdão n.º 403/2015 que, no seu ponto 10, refere:

«Após o primeiro diploma, que estabeleceu os princípios gerais das comunicações - o Decreto-Lei n.º 188/81, de 2 de julho –, as ulteriores Leis de Bases das Redes e Prestação de Serviços de Telecomunicações - Lei n.º 88/89, de 11 de setembro e Lei n.º 91/97, de 1 de agosto - preocuparam-se em regular o tratamento dos dados pessoais gerados pelas telecomunicações. Nesta última Lei previa-se expressamente, no n.º 2, do artigo 17.º uma cláusula destinada a garantir a inviolabilidade e o sigilo dos serviços de telecomunicações de uso público, nos termos da lei.

Entretanto, foi aprovada a Lei de Proteção de Dados Pessoais - Lei n.º 67/98, de 26 de outubro -, que se destinou a transpor para a ordem jurídica portuguesa a Diretiva 95/46/CE do Parlamento e do Conselho, de 24 de outubro de 1995, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Posteriormente, a Lei n.º 69/98, de 28 de outubro – que transpôs a Diretiva 97/66/CE, do Parlamento Europeu e do Conselho –, veio regular o tratamento de dados pessoais e a proteção da privacidade no setor das telecomunicações, especificando e complementando as disposições da Lei da Proteção de Dados. Esse diploma impõe ao prestador de serviços de telecomunicações o dever de adotar todas as medidas técnicas e organizacionais necessárias para garantir a segurança desses serviços de telecomunicações, impondo também aos operadores de rede o dever de garantir a confidencialidade e o sigilo das telecomunicações, através dos serviços acessíveis ao público e das redes públicas de telecomunicações.

Os Decretos-Lei n.º 290-A/99 e 290-B/99, ambos de 30 de julho, vieram consagrar, como 'obrigações dos operadores de redes públicas de telecomunicações', a proteção de dados e o sigilo das comunicações suportadas na rede que exploram e a de assegurar o sigilo das comunicações do serviço prestado, bem como o disposto na legislação de proteção de dados.

A introdução de novas tecnologias digitais nas redes de comunicações públicas trouxe consigo uma grande capacidade e possibilidade de tratamento de dados pessoais, e determinou a necessidade de acautelar novos requisitos específicos de proteção de dados pessoais e da privacidade dos utilizadores. De facto, os novos meios de comunicação, disponíveis a um custo cada vez menor e acessíveis a um número cada vez maior de pessoas vieram multiplicar os riscos para a privacidade dos seus utilizadores. Tal facto justificou que a Diretiva 97/66/CE fosse revogada e substituída pela Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

O objetivo deste novo regime foi estender a proteção oferecida pela anterior Diretiva aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas. Especificamente no que respeita aos dados de tráfego, a Diretiva define-os como 'quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma, e 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, ou ao formato revestido pela mesma'. A normativa europeia estabelece, em particular, regras referentes à eliminação dos dados, exigindo, para a sua conservação, o respeito pelo princípio da proporcionalidade. Nesse ponto, refere-se que 'a eliminação dos dados de tráfego justifica-se pela sua especial sensitividade, que poderia permitir elaborar e revelar o perfil da comunicação, dando a conhecer, v.g. a sua origem geográfica' (Catarina Sarmento e Castro, ob. cit, pág. 172).

E, assim, mercê do dever de transposição desta nova diretiva europeia, a referida Lei n.º 69/98 foi revogada pela Lei n.º 41/2004, de 18 de agosto, a qual veio aprovar o regime jurídico do tratamento

de dados pessoais e da proteção da privacidade no setor das comunicações eletrónicas. Este último diploma legal preocupou-se especialmente com a faturação detalhada e a localização celular. Em conformidade com a diretiva europeia transposta, a Lei n.º 41/2004 não prejudica a possibilidade de existência de legislação especial que restrinja a sua aplicação no que respeita à inviolabilidade das comunicações, nomeadamente para efeito de investigação e repressão de infrações penais (artigo 1.º, n.º 4).

Assim, na sequência desse diploma, foi aprovada a Lei n.º 32/2008, de 17 de julho que transpôs para a ordem jurídica interna a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15/03, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, que estabelece amplas garantias no que toca ao acesso e conservação dos dados de tráfego e de localização das comunicações para fins de investigação, deteção e repressão de crimes graves por parte das autoridades.»

É de referir também que, posteriormente, foi aprovada a Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), transpondo para a ordem jurídica nacional a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa. O n.º 2 do artigo 11.º da Lei do Cibercrime vem estabelecer que as disposições processuais previstas no capítulo III daquela lei «não prejudicam o regime da Lei n.º 32/2008, de 17 de julho».

8. Também é importante referir o enquadramento internacional da questão. Sobre a mesma, o Acórdão n.º 403/2015, no seu ponto 11, elenca:

«Assim, desde logo, o artigo 12.º da Declaração Universal dos Direitos do Homem declara que 'ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência (…)'. A mesma redação é retomada pelo artigo 17.º do Pacto Internacional relativo aos Direitos Civis e Políticos. Ambos os textos prescrevem que o indivíduo tem direito à proteção da lei contra tais intervenções ou tais atentados.

O artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH), por seu turno, estabelece que 'qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência'. Nos termos do n.º 2, 'não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros'. O Tribunal Europeu dos Direitos do Homem (TEDH) tem desenvolvido uma ampla jurisprudência sobre a proteção do acesso a dados de comunicações, afirmando expressamente que os mesmos se encontram abrangidos pela proteção de 'vida privada e familiar' ínsita no n.º 1 do artigo 8.º da CEDH. Assim, no caso Malone c. Reino Unido, referiu que o acesso e uso de dados respeitantes a tráfego de comunicações constituem matéria que é abrangida pelo âmbito de proteção do n.º 1 do artigo 8.º da CEDH (Acórdão de 02/08/1984, queixa n.º 8691/79).

Por fim, no contexto da União Europeia, cabe mencionar os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. Note-se que, antes de a mesma produzir efeitos vinculativos, o

Tribunal de Justiça da União Europeia já havia proclamado a existência de um 'princípio geral de direito comunitário que consagra a proteção contra as intervenções arbitrárias e desproporcionadas do poder público na esfera da atividade privada de uma pessoa singular ou coletiva' (Acórdão de 22/10/2002, Roquette Frèrres, processo n.º C-94/00). Atualmente, o artigo 7.º da Carta dos Direitos Fundamentais consagra o respeito pela vida privada e familiar, dispondo, inspirado nas demais normas internacionais, que 'todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações'. Este direito vale, nos termos do artigo 52.º, n.º 3 da Carta, com o mesmo sentido que é conferido ao artigo 8.º da CEDH. Por seu turno, o artigo 8.º da Carta contém uma norma específica relativa à proteção de dados pessoais, proteção essa que recebe, assim, uma consagração expressa e autónoma face ao artigo 7.º. A norma em causa estabelece que 'todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito'. O Tribunal de Justiça da União referiu que este direito está 'indissociavelmente relacionado com o direito ao respeito pela vida privada' (Acórdão de 09/11/2010, Volkerund Markus Schecke, processo n.º C-92/09 e C-93/09). Por outro lado, esclareceu que a proteção de dados de tráfego das comunicações se encontra abrangida pelo âmbito de proteção deste direito fundamental (assim, o Acórdão de 08/04/2014, Digital Rights Ireland Ltd., processos n.º C-293/12 e C-594/12, que, anulou a Diretiva 2004/26/CE, por violação dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais).»

Este último Acórdão do Tribunal de Justiça no caso *Digital Rights Ireland* (Proc. n.º C-293/12 e C-594/12) é especialmente relevante neste enquadramento, como se verá de seguida.

c) Apreciação da questão de constitucionalidade

9. O despacho de 19 de outubro de 2016 que indeferiu o pedido do Ministério Público de autorização de transmissão dos dados de identificação de um utilizador a quem estava atribuído um determinado endereço de protocolo IP teve como fundamento a inconstitucionalidade do artigo 6.º da Lei n.º 32/2008, por referência ao artigo 4.º da mesma lei.

Essa inconstitucionalidade é sustentada através da invocação do Acórdão do Tribunal de Justiça *Digital Rights Ireland* (Proc. n.º C-293/12 e C-594/12) que declarou a invalidade da Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Este ato normativo foi transposto para a ordem jurídica da República Portuguesa pela Lei n.º 32/2008, de 17 de julho, diploma onde se insere a norma objeto do presente processo.

No despacho considera-se que a maioria das considerações do Tribunal de Justiça seria aplicável a uma apreciação da Lei n.º 32/2008. Refere que apenas as relativas «às condições do posterior aproveitamento dos dados conservados e (…) ao grau de segurança relativa dos dados, (…) poderiam não ser incluídos na referência à solução apresentada pela Lei n.º 32/2008» (p. 9 do despacho, fls. 43).

Considera, por isso, que «a conservação de dados é determinada na Lei n.º 32/2008 com a mesma amplitude, generalidade, injustificação, ausência de controle prévio na inserção de dados e duração excessiva, de forma desproporcionada, que resultavam da Diretiva» (p. 9 do despacho, fls. 43). Daqui decorreria «a contrariedade (…) do regime legal instituído pela Lei n.º 32/2008, especificamente do seu artigo 6.º, com o disposto no artigo 8.º da Convenção Europeia dos Direitos do Homem e nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, de forma paralela ao referido no Acórdão do Tribunal de Justiça (…) de 8 de abril de 2014» (p. 10 do despacho, fls. 44). Também seria de aceitar esta lógica por referência aos artigos 18.º e 34.º da Constituição, especificamente o n.º 4 deste último preceito. Por esse motivo, «a imposição de preservação de todo o tipo de dados referente à vida privada dos utilizadores de serviços de telecomunicação, sem qualquer restrição, durante um ano, sem qualquer ligação a um procedimento penal, automática, sem qualquer controlo jurisdicional prévio, com o risco de acesso por qualquer pessoa no fornecedor desses serviços (…), sem referência a um concreto perigo e uma classe grave de infrações, mostra-se ser desproporcionada em relação à reserva da vida privada» (p. 10-11 do despacho, fls. 44-45). Recusa, assim, a aplicação «do disposto no artigo 6.º da Lei n.º 32/2008 (por referência ao artigo 4.º da mesma Lei) por contrariedade aos artigos 18.º e 34.º, n.º 4, da Constituição» (cfr. a alínea *a)* da decisão do despacho, fls. 45)

10. Começa por se referir que a declaração de invalidade de uma diretiva não tem uma consequência automática sobre a validade de um ato legislativo português que a transponha. O ato legislativo nacional, embora tendo como objetivo o cumprimento do dever de transposição de uma diretiva, decorrente do Direito da UE (artigo 4.º, n.º 3, do Tratado da EU, artigo 288.º, 3.º parágrafo, do Tratado sobre o Funcionamento da EU e artigo 112.º, n.º 8, da Constituição), tem uma fonte autónoma de validade e legitimidade.

O Tribunal de Justiça não tem jurisdição para apreciar a validade dos atos de direito nacional dos Estados-Membros, sendo que a sua análise apenas incidiu sobre o texto da diretiva. A validade da Lei n.º 32/2008, de 17 de julho, não pode ser posta em causa apenas devido ao facto de este ato normativo da União ter sido declarado inválido.

Tais considerações não impedem, no entanto, que se proceda à fiscalização da validade dessa Lei à luz dos parâmetros aplicáveis, nomeadamente de Direito Internacional, previstos na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de Direito da União Europeia, consagrados na Carta dos Direitos Fundamentais da União Europeia, ou de direito nacional, decorrentes da Constituição. Embora seja de ter em conta, nesse processo, a fundamentação do Tribunal de Justiça, este juízo deverá ser, no entanto, autónomo relativamente ao efetuado por esta instância jurisdicional.

No presente processo, ao desempenhar essa tarefa, não é possível acompanhar o raciocínio explanado na decisão recorrida.

11. Desde logo porque um conjunto de considerações tecidas pelo Tribunal de Justiça não pode ser importado, sem mais, para a fiscalização da Lei n.º 32/2008 e para o presente processo.

Esta lei, ao transpor a Diretiva n.º 2006/24/CE, densificou-a, consagrando soluções jurídicas que merecem uma análise específica. A mero título de exemplo, a Lei n.º 32/2008 prevê a obrigação de os operadores de comunicações conservarem os dados abrangidos pelo seu âmbito pelo período de

um ano, enquanto a Diretiva estabelecia a sua conservação «por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação» a estabelecer pelos Estados-Membros (artigo 6.º da Diretiva n.º 2006/24/CE). A este respeito, referem DAVID SILVA RAMALHO e JOSÉ DUARTE COIMBRA ("A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", *in* O Direito, n.º 147.º (2015), IV, pp. 997-1045, pp. 1037-1038):

«Recorde-se que, entre os fundamentos apresentados pelo TJ para a declaração de invalidade da Diretiva, encontravam-se (i) a ausência de normas substantivas ou processuais que determinem o critério de acesso aos dados; (ii) a ausência de definição do conceito de "crimes graves"; (iii) a não consagração de reserva de juiz; (iv) a inexistência de garantias de segurança na conservação e transmissão dos dados; (v) a sua aplicação a pessoas sujeitas a segredo profissional; (vi) e a omissão de imposição da conservação dos dados em território da União Europeia.

Ora, ao transpor a Diretiva para o ordenamento jurídico nacional, o legislador português (i) estipulou regras de acesso aos dados, sujeitando-o a critérios de necessidade, adequação e proporcionalidade, a verificar inclusivamente no que respeita à definição das categorias de dados (n.ºs 1 e 4 do artigo 9.º) e limitando-o a um catálogo restrito de titulares dos dados (n.º 3 do artigo 9.º); (ii) definiu o conceito de crimes graves (alínea g) do n.º 1 do artigo 2.º); (iii) impôs a precedência de mandado judicial no acesso aos dados, mediante requerimento do Ministério Público ou da autoridade de polícia criminal competente (n.º 2 do artigo 9.º); (iv) estabeleceu particulares deveres de proteção e segurança dos dados, tendo, inclusivamente, criado uma aplicação informática denominada «sistema de acesso ou pedido de dados às operadoras de comunicações» (SAPDOC), por onde o processo de transmissão e acesso aos dados decorre, através de ligação segura, encriptada mediante nome de utilizador e palavra passe, através de obrigação de registo eletrónico dos pedidos de dados enviados, incluindo a indicação de quem procedeu ao envio e da data e hora em que o mesmo ocorreu, bem como dos acessos a ficheiros de resposta, igualmente com indicação de quem os efetuou e da data e hora de cada acesso (n.º 3 do artigo 7.º da Lei n.º 32/2008 e Portaria n.º 469/2009); e (v) sujeitou expressamente a decisão judicial de transmitir os dados ao dever de respeitar o segredo profissional nos termos legalmente previstos, apesar de não evitar a sua conservação (n.º 4 do artigo 9.º). (…)»

Na Nota Prática n.º 7/2015, de 30 de dezembro de 2015, sobre Retenção de dados de tráfego e Lei n.º 32/2008, de 17 de julho, o Gabinete do Cibercrime do Ministério Público esclarece igualmente (n.º 5):

«É importante sublinhar que a Lei n.º 32/2008, além da transposição da Diretiva 2006/24/CE, introduziu um mais alargado quadro, muito complexo, de regulamentação do processo de retenção de dados (por exemplo, entre outras, as regras que devem ser observadas na retenção, as pessoas habilitadas a aceder os dados ou as condições de armazenamento e de acesso aos dados). Neste exercício, a lei nacional foi muito para lá das exigências da Diretiva. Desta forma, a maior parte das exigências que vieram a ser feitas pelo acórdão do TJUE estariam já anteriormente consideradas no direito interno. Por essa razão, tem sido entendido que a decisão do tribunal do Luxemburgo não afeta a validade da lei nacional.

Como exemplo do que se disse, a lei portuguesa estipula condições de acesso aos dados, exigindo que a divulgação seja precedida de ordem de um juiz (Artigo 9.º, n.º 1, da Lei n.º 32/2008). Esta condição coincide com a exigência do Tribunal de Justiça, quando declara e tira consequências

negativas do facto de a Diretiva não prever, no acesso aos dados, a exigência de autorização de uma autoridade independente.

Por outro lado, o Tribunal valora negativamente a circunstância de a Diretiva não prever a obrigação de destruir os dados após o período de retenção. A lei portuguesa estatui exatamente o oposto, impondo a destruição dos dados após o período de retenção (artigo 7.º, n.º 1, alínea e, da Lei n.º 32/2008).

Em relação à conservação dos dados, o TJUE sublinhou também a falta de requisitos reguladores da mesma. Mais uma vez, a lei portuguesa prevê regras que traduzem importantes salvaguardas a este propósito (por exemplo, definindo quem são aqueles que estão autorizados a aceder os dados, as estritas condições de armazenamento e outros).»

Sendo as soluções nacionais distintas da norma da União, um juízo sobre a sua constitucionalidade deve ter em conta essas diferenças.

É de notar que o Acórdão do Tribunal de Justiça *Digital Rights Ireland* (Proc. n.º C-293/12 e C-594/12), invocado pela decisão recorrida, incide a sua análise nomeadamente sobre o dever de conservação dos dados de tráfego e de localização, considerados no seu todo (cfr. n.os 17, 27, 32, 56-57), não exatamente sobre os dados de base, como acontece no presente processo. O enfoque especial dado no Acórdão *Digital Rights Ireland* (Proc. n.º C-293/12 e C-594/12) aos dados de tráfego já tinha sido notado pelo Tribunal Constitucional no Acórdão n.º 403/2015, ponto 15:

«o Tribunal de Justiça da União (…), no já referido Acórdão de 08/04/2014, Digital Rights Ireland Ltd., processos n.º C-293/12 e C-594/12, que anulou a Diretiva 2004/26/CE, referiu ilustrativamente que, no que toca aos dados de tráfego das comunicações, 'a conservação dos dados imposta pela Diretiva 2006/24 constitu[i] uma ingerência particularmente grave nesses direitos», embora não seja «suscetível de afetar o referido conteúdo, tendo em conta que, como resulta do seu artigo 1.º, n.º 2, esta diretiva não permite tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal' (parágrafo 39). O TJ sublinhou várias vezes a gravidade da ingerência resultante de uma conservação ilimitada de dados de tráfego, pelo facto de os mesmos permitirem 'designadamente, saber qual é a pessoa com quem um assinante ou um utilizador registado comunicou, e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Além disso, permitem saber com que frequência o assinante ou o utilizador registado comunicam com certas pessoas, durante um determinado período' (parágrafo 26). Mais afirmou: 'estes dados, considerados no seu todo, são suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados' (parágrafo 27). Assim, conclui, inter alia, que 'apesar de a Diretiva 2006/24 não autorizar (…) a conservação do conteúdo da comunicação e das informações consultadas através de uma rede de comunicações eletrónicas, não está excluído que a conservação dos dados em causa possa ter incidência na utilização, pelos assinantes ou pelos utilizadores registados, dos meios de comunicação previstos por esta diretiva e, consequentemente, no exercício, por estes últimos, da sua liberdade de expressão, garantida pelo artigo 11.º da Carta' (considerando 28)» (sublinhado aditado).

A mesma conclusão pode ser retirada do recente Acórdão do Tribunal de Justiça *Tele2 Sverige* (Proc. n.º C-203/15 e C-698/15), de 21 de dezembro de 2016 (cfr. n.os 92, 99, 102-105, 110, 112, 114 e 125).

Assim, não é correto basear a invalidade da lei nacional numa transposição do juízo efetuado pelo Tribunal de Justiça sobre a globalidade do texto da diretiva que esta transpõe, sem proceder a uma análise específica e autónoma da norma nacional que esteja em causa e, no presente caso, sem atender à natureza dos dados de base.

12. No caso, o principal obstáculo que o juízo de inconstitucionalidade do despacho recorrido enfrenta é a correta delimitação da norma objeto de fiscalização de constitucionalidade. Na verdade, a norma que é dada a fiscalizar abrange exclusivamente o dever de os fornecedores de serviços de comunicações eletrónicas conservarem, durante um período de tempo, os dados de base. É o julgamento dessa norma específica que nos deve ocupar.

O Tribunal Constitucional já teve oportunidade de se pronunciar, embora indiretamente, quanto ao regime de proteção constitucional dos dados de base.

No Acórdão n.º 486/2009 esclarece o Tribunal Constitucional, no seu ponto 2.2:

«O sigilo das telecomunicações, garantido nos termos do artigo 34.º, n.º 1, da Constituição, abrange não só o conteúdo das comunicações mas também o tráfego como tal (V. GOMES CANOTILHO/VITAL MOREIRA, ob.cit.. pág. 538 e segs.).

'O que está em causa é assegurar o livre desenvolvimento da personalidade de cada um através da troca à distância, de informações, notícias, pensamentos e opiniões, à margem da devassa da publicidade' (COSTA ANDRADE, em 'Bruscamente no verão passado..., Ano 137.º, n.º 3951, Julho-Agosto 2008, p. 339).

A privacidade da comunicação, como corolário da reserva da intimidade da vida privada, abrange não apenas a proibição de interferência, em tempo real, de uma chamada telefónica, como também a impossibilidade do ulterior acesso de terceiros a elementos que revelem as condições factuais em que decorreu uma comunicação (…).

Efetivamente, num Estado de Direito democrático, assiste a qualquer cidadão o direito de telefonar quando e para quem quiser com a mesma privacidade que se confere ao conteúdo da sua conversa.

O mesmo raciocínio não vale para os elementos ou dados de base, já que, conforme assinala COSTA ANDRADE 'a pertinência dos dados à categoria e ao regime das telecomunicações pressupõe, em qualquer caso, a sua vinculação a uma concreta e efetiva comunicação – ao menos tentada/falhada – entre pessoas' (ob. cit., p. 341),

Na verdade, por exemplo, a mera identificação do titular de um número de telefone fixo ou móvel, mesmo quando confidencial, surge com uma autonomia e com uma instrumentalidade relativamente às eventuais comunicações e, por isso mesmo, não pertence ao sigilo das telecomunicações, nem beneficia das garantias concedidas ao conteúdo das comunicações e aos elementos de tráfego gerados pelas comunicações propriamente ditas (Vide, neste sentido, COSTA ANDRADE, em 'Comentário Conimbricense do Código Penal', Parte Especial, Tomo III, pág. 797-798, da ed. de 2001, da Coimbra Editora).

A mesma falta de tutela constitucional no plano do sigilo das telecomunicações valerá para os dados de localização celular que não pressuponham qualquer ato de comunicação, bastando para o efeito que o telemóvel esteja em posição de stand by, isto é, ligado e apto para receber chamadas (Vide, neste sentido COSTA ANDRADE, em 'Bruscamente no verão passado..., Ano 137.º, n.º 3951, julho-agosto 2008, p. 341)» (sublinhado aditado).

Também no Acórdão n.º 403/2015, ponto 15, se refere que:

«(…) há um largo consenso na doutrina e na jurisprudência, de resto não se conhece posição contrária, no sentido de se incluir os dados de tráfego no conceito de comunicações constitucionalmente relevante para a proibição de ingerência. Quer dizer: o âmbito de proteção do artigo 34.º, n.º 4 abrange não apenas o conteúdo das telecomunicações, mas também os dados de tráfego.

(…)

O Tribunal Constitucional também já teve oportunidade de se pronunciar expressamente sobre este aspeto, tendo também equiparado a proteção dos dados de tráfego à proteção constitucionalmente concedida aos dados de conteúdo. Assim, no Acórdão n.º 241/02, em que refere expressamente que 'a proibição de ingerência nas telecomunicações, para além de vedar a escuta, interceção ou vigilância de chamadas, abrange, igualmente, os elementos de informação com elas conexionados, designadamente os que no caso foram fornecidos pelos operadores de telecomunicações'. A mesma interpretação foi retomada e amplamente desenvolvida no Acórdão n.º 486/2009 (…).

(…)

Já quanto aos dados de base (v.g. número de telefone, endereço eletrónico, contrato de ligação à rede) e aos dados de localização de equipamento, quando não dão suporte a uma concreta comunicação, não são objeto de proteção do direito ao sigilo das comunicações (cfr. Acórdão n.º 486/2009). De facto, se o objeto de proteção é uma comunicação individual, então os dados que não pressuponham uma concreta comunicação, que não façam parte do processo de comunicação, ainda que protegidos pela reserva da vida privada – artigo 26.º da CRP – não estão cobertos pela tutela do sigilo das comunicações.

Por tudo isso, também se entende que a área de proteção do sigilo das comunicações consagrada no n.º 4 do artigo 34.º da CRP, compreende tanto o conteúdo da comunicação como os dados de tráfego atinentes ao processo de comunicação. (…)»

Esta diferença de tratamento também tem reflexos nos outros tribunais, levando a que «os tribunais superiores da jurisdição comum tenham vindo a conferir um tratamento diverso, no sentido de uma menor proteção – *rectius*, uma menos acentuada intangibilidade –, aos dados de base, colocando-os no plano das demais informações sujeitas a segredo profissional, nos termos do artigo 135.º do CPP (cfr. os acórdãos do Tribunal da Relação de Lisboa de 19/06/2014, proferido no processo n.º 1695/09.5PJLSB.L1-9, de 20/06/2013, proferido no processo n.º 1746/05.2TJLSB.L1-8, e de 18/01/2011, proferido no processo n.º 3142/09.3PBFUN-A.L1-5, todos disponíveis na base de dados da DGSI)» (cfr. ponto 9.2 do voto do Cons. José António Teles Pereira ao mesmo Acórdão n.º 403/2015).

Assim, decorre da jurisprudência do Tribunal Constitucional sobre esta matéria que a proteção conferida pelo n.º 4, do artigo 34.º da Constituição não abrange os dados de base, como os abrangidos pela norma objeto do presente processo. De facto, os dados relativos à mera identificação de um utilizador a quem estava atribuído um determinado endereço de protocolo IP não estão abrangidos pelo âmbito de proteção do sigilo das comunicações consagrado naquele preceito constitucional pois não pressupõe um ato de comunicação específico. Não se acompanha, portanto, o juízo do tribunal *a quo*, quanto à violação do n.º 4 do artigo 34.º da Constituição.

13. Os dados de base em causa estão, no entanto, sujeitos à proteção concedida pelo direito à reserva da vida privada, consagrado no artigo 26.º da Constituição.

Assim sendo, é necessário aferir se a obrigatoriedade de os «fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações» conservarem «pelo período de um ano a contar da data da conclusão da comunicação», os dados relativos ao «nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP» estava atribuído «no momento da comunicação» constitui uma restrição destes direitos fundamentais e se tal restrição é desproporcionada, violando o artigo 18.º da Constituição.

Ora, o dever de conservação destes dados para a sua eventual disponibilização às autoridades, nos termos da lei, pode ser vista como uma restrição aos direitos fundamentais referidos. A questão coloca-se, pois, na sua conformidade com o princípio da proporcionalidade.

O princípio da proporcionalidade ocupa lugar central na avaliação dos requisitos materiais exigidos nas restrições de direitos fundamentais que, de acordo com o n.º 2, do artigo 18.º da Constituição, devem «limitar-se ao necessário para salvaguardar outros direitos e interesses constitucionalmente protegidos». Importa, pois, começar por identificar o interesse público prosseguido pela norma sindicada. No presente caso, o interesse público é a «investigação, deteção e repressão de crimes graves por parte das autoridades competentes», tal como previsto no artigo 1.º, n.º 1, da Lei n.º 32/2008. Os crimes graves são definidos como «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» (artigo 2.º, n.º 1, alínea *g)*, da Lei n.º 32/2008). A salvaguarda da legalidade democrática e a ação penal, nomeadamente contra os crimes referidos, constituem interesses públicos com proteção constitucional.

São comumente identificados os seguintes três subprincípios em que se desdobra o princípio da proporcionalidade: idoneidade (ou adequação), necessidade (ou indispensabilidade) e justa medida (ou proporcionalidade em sentido estrito).

Ora, a medida em causa cumpre os requisitos de idoneidade, pois a conservação de dados de base é uma medida adequada para permitir a identificação do utilizador registado, a quem o endereço do protocolo IP estava atribuído, suspeito de autoria de um dos crimes graves referidos, e de necessidade, na medida em que não é possível configurar um meio menos restritivo para as autoridades competentes procederem à referida identificação.

O princípio da proporcionalidade em sentido estrito veda a adoção de medidas que se apresentem como excessivas (desproporcionadas) para atingir os fins visados. Neste juízo é necessário ponderar, de um lado, a natureza relativamente pouco invasiva da privacidade dos dados

em questão (dados de base), dizendo respeito à identidade do utilizador, e o período temporal de conservação (um ano) – após o qual os dados são destruídos (artigo 7.º, n.º 1, alínea *e)*, da Lei n.º 32/2008), tendo em conta, por outro lado, a natureza especialmente grave dos crimes em questão e a centralidade destes dados para a condução da investigação criminal. Também é de ter em atenção o regime previsto para o acesso a estes dados, com limitação do universo de titulares de dados sujeitos à transmissão (artigo 9.º, n.º 3, da Lei n.º 32/2008), e impondo a necessidade de autorização prévia, por despacho fundamentado do juiz de instrução, que deve respeitar os princípios da adequação, necessidade e proporcionalidade, a requerimento do Ministério Público ou da autoridade de polícia criminal competente (artigo 9.º, n.os 1, 2 e 4, da Lei n.º 32/2008). Por esses motivos, a norma objeto do presente recurso não viola o princípio da proporcionalidade decorrente do artigo 18.º, n.º 2, da Constituição.

14. É, assim, de concluir pela não desproporcionalidade da restrição ao direito à proteção da vida privada decorrente da norma que estabelece o dever de os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações conservarem pelo período de um ano a contar da data da conclusão da comunicação, os dados relativos ao nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP estava atribuído no momento da comunicação, constante do disposto no artigo 6.º e do artigo 4.º, n.º 1, alínea *a)*, 2.ª parte, e n.º 2, alínea *b)*, subalínea *iii)*, ambos da Lei n.º 32/2008 de 17 de julho.

III. Decisão

Termos em que se decide:

a) Não julgar inconstitucional a norma que estabelece o dever de os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações conservarem pelo período de um ano a contar da data da conclusão da comunicação, os dados relativos ao nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP estava atribuído no momento da comunicação, constante do disposto no artigo 6.º e do artigo 4.º, n.º 1, alínea *a)*, 2.ª parte, e n.º 2, alínea *b)*, subalínea *iii)*, ambos da Lei n.º 32/2008 de 17 de julho;

b)Em consequência, conceder provimento ao recurso, ordenando-se a reforma da decisão recorrida em conformidade com o presente juízo de não inconstitucionalidade.

Sem custas.

Lisboa 13 de julho de 2013 - *Maria de Fátima Mata-Mouros* - *João Pedro Caupers* - *Claudio Monteiro* - *José Teles Pereira* - *Manuel da Costa Andrade*