Exmo. Senhor Presidente do Tribunal Constitucional
Juiz Conselheiro Manuel da Costa Andrade

Q/7746/2017

A Provedora de Justiça vem, ao abrigo do disposto no artigo 281.º, n.º 1, alínea *a)*, e n.º 2, alínea *d)*, da Constituição da República Portuguesa, requerer ao Tribunal Constitucional a fiscalização abstrata da constitucionalidade dos artigos 4.º, 6.º e 9.º, da Lei n.º 32/2008, de 17 de Julho, que transpõe para a ordem jurídica interna a Directiva 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações, por violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1) e ao sigilo das comunicações (artigo 34.º, n.º 1) e por violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1).

A. A relação entre a Lei n.º 32/2008, de 17 de Julho, e o direito da União Europeia

1.º

Nos termos do disposto no artigo 6.º da Lei n.º 32/2008, de 17 de julho, os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações têm o dever de conservar, pelo período de um ano, os dados de tráfego e de localização de todas as comunicações electrónicas, os quais vêm especificados no artigo 4.º do mesmo diploma.

2.º

Trata-se dos dados relativos às subscrições e a todas as comunicações electrónicas necessários para encontrar e identificar a fonte e o destino de uma comunicação (artigo 4.º, n.º 1, alíneas *a)* e *b)*), para determinar a data, a hora, a duração e o tipo de comunicação (artigo 4.º, n.º 1, alíneas *c)* e *d)*), para identificar o equipamento de telecomunicações dos utilizadores (artigo 4.º, n.º 1, alínea *e)*) e para identificar a localização do equipamento de comunicação móvel (artigo 4.º, n.º 1, alínea *f)*).

3.º

A obrigação de conservação dos dados abrange os dados gerados ou tratados no âmbito de um serviço telefónico na rede fixa, de um serviço telefónico na rede móvel, de um serviço de acesso à Internet, de um serviço de correio electrónico através da Internet bem como de um serviço de comunicações telefónicas através da Internet.

4.º

Esta obrigação também inclui os dados relativos às chamadas telefónicas falhadas (artigo 5.º, n.º 1).

5.º

Fora da obrigação de conservação dos dados estão os dados relativos ao conteúdo das comunicações, porquanto, nos termos do disposto no n.º 2 do artigo 1.º, a conservação de tais dados é expressamente proibida.

6.º

No que diz respeito às comunicações telefónicas na rede fixa devem ser conservados os dados relativos ao número de telefone de origem e aos números marcados, os dados relativos ao nome e endereço dos assinantes ou dos utilizadores registados (artigo 4.º, n.º 2, alínea *a)* e n.º 3, alínea *a)*), os dados relativos à data e hora do início e do fim da comunicação (artigo 4.º, n.º 4, alínea *a)*), os dados relativos ao serviço telefónico utilizado (artigo 4.º, n.º 5, alínea *a)*) e os números de telefone de origem e de destino (artigo 4.º, n.º 6, alínea *a)*). Relativamente às comunicações telefónicas na rede móvel, aplicam-se obrigações suplementares, tais como a conservação da Identidade Internacional de Assinante Móvel (IMSI) e da Identidade Internacional de Equipamento

Móvel (IMEI) de quem telefona e do destinatário (artigo 4.º, n.º 6, alínea *b)*), bem como dos dados de localização do início e do fim da comunicação (artigo 4.º, n.º 7).

7.º

No que diz respeito aos serviços de acesso à Internet, aos serviços de correio electrónico através da Internet e às comunicações telefónicas através da Internet devem ser conservados os códigos de identificação atribuídos ao utilizador, o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública e o nome e 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 (artigo 4.º, n.º 2, alínea *b)*), bem como as datas e horas do início (*log in*) e do fim (*log off*) da ligação ao serviço de acesso à Internet ou da ligação, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado (artigo 4.º, n.º 4, alínea *b)*, subalínea *i)*) ou da ligação ao serviço de correio electrónico através da Internet (artigo 4.º, n.º 4, alínea *b)*, subalínea *ii)*), o serviço de Internet utilizado (artigo 4.º, n.º 5, alínea *b)*) e ainda os dados relativos ao número de telefone que solicita o acesso por linha, a linha de assinante digital ou qualquer outro identificador terminal do autor da comunicação (artigo 4.º, n.º 6, alínea *c)*).

8.º

Em causa estão, portanto, dados que revelam a todo o momento aspectos da vida privada e familiar dos cidadãos, permitindo rastrear a localização do indivíduo ao longo do dia, todos os dias (desde que transporte o telemóvel ou outro dispositivo electrónico de acesso à Internet), e identificar com quem contacta (chamada – inclusive as tentadas e não concretizadas – por telefone ou telemóvel, envio ou recepção de SMS, MMS, de correio electrónico, ou de comunicações telefónicas através da Internet), bem como a duração e a regularidade dessas comunicações.

9.º

A Lei n.º 32/2008, de 17 de julho, transpôs para a ordem jurídica nacional a Directiva 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações.

10.º

O Tribunal de Justiça da União Europeia (TJUE) declarou a invalidade da referida Directiva no acórdão de 8 de abril de 2014, *Digital Rights Ireland Ltd e outros*, C-293/12 e C-594/12.

11.º

A declaração de invalidade teve por fundamento a violação do princípio da proporcionalidade pela restrição que a Directiva opera dos direitos ao respeito pela vida privada e familiar e à protecção de dados pessoais, consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (Carta).

12.º

Com efeito, apesar de o TJUE ter reconhecido que as medidas previstas na Directiva – relativas à imposição do dever de conservação de dados de tráfego e de localização gerados no contexto de comunicações electrónicas e ao dever da sua transmissão às autoridades competentes para efeitos de investigação, detecção e repressão de crimes graves – eram, em si mesmas, medidas legítimas e adequadas ao fim visado, nem por isso deixou de concluir que as mesmas violavam o princípio da proporcionalidade, na sua dimensão de [do subprincípio da] *necessidade*.

13.º

Tratando-se de um acto de transposição de uma directiva, a Lei n.º 32/2008, de 17 de julho, consubstancia, para efeitos do disposto no n.º 1 do artigo 51.º da Carta, um acto de aplicação do direito da União Europeia.

14.º

Tal significa que, embora tratando-se formalmente de legislação nacional e não de um acto adoptado pelas instituições da União Europeia, a Lei n.º 32/2008, de 17 de julho, está directamente vinculada pela Carta.

15.º

Nesta medida, os fundamentos invocados pelo TJUE para sustentar a declaração de invalidade do regime europeu que a Lei n.º 32/2008 pretendeu transpor não poderão deixar de ser tidos em conta, no momento em que se afira da conformidade ou não conformidade em relação à Carta das normas contidas neste regime nacional.

16.º

Além disso, resulta do acórdão do TJUE de 21 de dezembro de 2016, *Tele2 Sverige e Watson*, C-203/15 e C-698/15, que qualquer legislação nacional que preveja a conservação de dados implica necessariamente a existência de disposições relativas ao acesso, por parte

das autoridades nacionais competentes, aos dados que sejam conservados pelos prestadores de serviços de comunicações eletrónicas. Assim, e ainda que a Directiva 2006/24 tenha sido declarada inválida pelo TJUE, nem por isso a Lei n.º 32/2008, de 17 de julho, poderá deixar de ser incluída no âmbito de aplicação da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (cfr. acórdão *Tele2*, n.os 79-81).

17.º

Pelo que não restam dúvidas de que a Lei n.º 32/2008, de 17 de julho, se enquadra no âmbito de aplicação do direito da União, encontrando-se, portanto, a definição pela República Portuguesa do regime legal de conservação de dados de comunicações electrónicas directamente vinculada pela Carta (artigo 51.º, n.º 1 da Carta).

18.º

É justamente em virtude da vinculação da legislação nacional à Carta que, no seguimento das decisões do TJUE, a Comissão Nacional de Protecção de Dados (CNPD) emitiu a Deliberação n.º 641/2017, de 9 de Maio, onde expôs a sua perspectiva sobre a Lei n.º 32/2008, considerando que a mesma contém normas que prevêem a restrição ou ingerência nos direitos fundamentais ao respeito pela vida privada e pelas comunicações e à protecção dos dados pessoais com grande amplitude e intensidade, em

violação do princípio da proporcionalidade e, portanto, em violação do n.º 1 do artigo 52.º da Carta, bem como uma restrição desproporcionada dos direitos à reserva da intimidade da vida privada, à inviolabilidade das comunicações e à protecção de dados pessoais, em violação do disposto no n.º 2 do artigo 18.º da Constituição da República Portuguesa.

19.º

Face a esse seu entendimento, a CNPD, através da Deliberação n.º 1008/2017, de 18 de julho, decidiu desaplicar a Lei n.º 32/2008 nas situações que lhe sejam submetidas para apreciação.

20.º

Tendo em conta todos estes dados, poder-se-ia concluir estar-se perante legislação nacional «inteiramente determinada» – na acepção do acórdão do TJUE de 26 de fevereiro de 2013, *Åkerberg Fransson*, C-617/10, n.° 29 –, pelo direito da União Europeia, o que geraria dúvidas quanto à questão de saber se caberia ainda à jurisdição constitucional nacional – e não à jurisdição própria da União Europeia – efectuar a ponderação entre as razões de interesse público que poderiam determinar a conservação e armazenamento de dados por parte das operadoras de telecomunicações e a tutela de direitos fundamentais.

21.º

Parece no entanto legítimo sustentar-se que, neste domínio, o legislador nacional definiu com certa margem de liberdade o regime instituído pela Lei n.º 32/2008, pelo que a normação nela contida não deverá ser qualificada como «acção estadual inteiramente determinada pelo Direito da União» na acepção que da expressão faz o acórdão atrás citado. Assim sendo, não estará em causa a competência da jurisdição constitucional nacional para levar a cabo o controlo de compatibilidade entre as medidas naquela legislação previstas e os direitos fundamentais em causa, nomeadamente o direito à reserva da intimidade da vida privada e à protecção dos dados pessoais.

22.º

Todavia, sendo embora a legislação nacional em questão «não inteiramente determinada» pelo direito da União Europeia –, e podendo, nessa medida, os órgãos jurisdicionais nacionais aplicar os padrões nacionais de proteção dos direitos fundamentais – em caso algum poderá dessa aplicação resultar um nível de protecção menos elevado do que aquele garantido pela Carta (acórdãos do TJUE de 26 de fevereiro de 2013, *Melloni*, C-399/11, n.° 60 e *Åkerberg Fransson*, C-617/10, n.° 29).

23.º

Assim é, pelo facto de a Lei n.º 32/2008, atendendo ao que dispõe a Directiva 2002/58/CE do Parlamento e do Conselho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das

comunicações electrónicas, ser ainda – não obstante a declaração de invalidade da Directiva 2006/24/CE – um acto de aplicação do Direito da União, encontrando-se por isso, e como já se disse, directamente vinculada pela Carta dos Direitos Fundamentais da União Europeia (artigo 51.º, nº1, da Carta).

24.º

Ora, embora seja claro que a Lei n.º 32/2008 não padece de alguns dos vícios apontados pelo TJUE à Directiva 2006/24/CE, por outro lado, é também inequívoco que, em aspectos fundamentais do regime nele instituído, esse acto legislativo se não conforma com as exigências decorrentes do direito da União, tal como interpretado pelo TJUE.

25.º

O argumento principal em que se baseou o Tribunal Constitucional no acórdão n.º 420/2017, de 13 de Julho, seguindo de perto a Nota Prática n.º 7/2015 do Gabinete do Cibercrime do Ministério Público, é o de que a legislação nacional estabelece já muitas das exigências que não estavam garantidas na Directiva invalidada pelo TJUE, designadamente no que respeita aos requisitos de *acesso* aos dados conservados bem como no que se refere à *imposição da destruição dos dados* após o período de conservação.

26.º

No entanto, e ao contrário do que é sugerido pela interpretação feita neste aresto, resulta claramente dos acórdãos do TJUE que a circunstância de, no que respeita ao *regime de acesso* aos dados conservados, a lei nacional poder ir ao encontro das exigências da Carta, em nada releva para efeitos da questão da conformidade à Carta da medida de imposição legal de conservação dos dados em si mesma considerada.

27.º

Com efeito, o TJUE, que é o órgão jurisdicional com competência para determinar a correcta interpretação da Carta dos Direitos Fundamentais da União Europeia, nos acórdãos *Digital Rights Ireland* e *Tele2*, a que já se fez referência, parte da premissa básica segundo a qual existirão, neste domínio, *dois momentos distintos e autónomos* de agressão aos direitos fundamentais.

28.º

Num primeiro momento, logo com a imposição legal aos operadores de telecomunicações da obrigação de conservação de dados, ocorre já uma agressão – e uma agressão que, só por si, é *grave* (cfr. acórdão *Tele2*, n.^{os} 99 e segs.) – aos direitos fundamentais.

29.º

Ou seja, mesmo que a esses dados nenhuma entidade pública viesse, posteriormente, alguma vez a aceder, já se dera uma agressão grave aos direitos individuais pela mera existência e armazenamento dos dados por parte dos operadores de telecomunicações.

30.º

Por sua vez, num segundo momento, que é incerto, o acesso e utilização por parte das entidades públicas competentes consubstancia um nível diferente de agressão aos direitos fundamentais, que vem, por assim dizer, acrescer à agressão – que só por si já é *grave* – implicada pela mera existência e armazenamento desses dados, agressão essa que, por definição, já terá ocorrido «a montante», e que tem que satisfazer, também ela, exigências decorrentes do princípio da proporcionalidade.

31.º

Ora, tratando-se de dois níveis diferentes de agressão aos direitos, não é possível argumentar que o facto de a Lei n.º 32/2008 satisfazer, no que respeita ao *regime de acesso* aos dados conservados, as exigências decorrentes da Carta, serve para *salvar* ou *compensar* a afectação dos direitos implicada na própria imposição legal de conservação de dados. Perante a existência de dois momentos autónomos de agressão aos

direitos, não é de todo legítimo confundi-los de acordo com uma «lógica de compensação»[1].

32.º

Pelo contrário, uma dogmática correcta de direitos fundamentais exigirá que se analise, autonomamente, a conformidade constitucional de cada uma das agressões aos direitos, em nada podendo o regime de acesso e de utilização dos dados interferir na análise da conformidade constitucional, designadamente e no que respeita às exigências decorrentes do princípio da proporcionalidade, da agressão aos direitos implicada na própria imposição legal de conservação de dados.

33.º

No que respeita ao primeiro nível de agressão dos direitos, que se dá com a imposição legal de conservação de dados aos operadores de telecomunicações, e que consubstancia por si só uma agressão *grave* de liberdades fundamentais (acórdão *Tele2*, n.º 99 e segs.), o TJUE, nos acórdãos *Digital Rights Ireland* e *Tele2*, já referidos, estabeleceu exigências claras, desde logo quanto ao âmbito da obrigação de conservação de dados, que a Lei n.º 32/2008, pura e simplesmente, não cumpre.

[1] Veja-se, a este respeito, o acórdão *Tele2*, que expressamente rejeita os argumentos defendidos, no processo, pelo Advogado-Geral, e que seriam favoráveis a essa «lógica de compensação» (n.os 192-215 das Conclusões do Advogado-Geral Henrik Saugmandsgaard Øe, apresentadas em 19 de Julho de 2016).

34.º

Na verdade, e quanto ao *âmbito da obrigação de conservação de dados* impendente sobre os operadores de telecomunicações, o legislador português acolhe a solução que o TJUE *expressamente* censurou: prevê uma conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica, sem limitar tal obrigação em função dos critérios indicados pelo TJUE nos termos do parágr. 106 e seguintes do acórdão *Tele2*.

35.º

Recorde-se que, tendo sido chamado a interpretar legislação nacional de Estados-Membros da União Europeia (Suécia e Reino Unido) que transpunha a Directiva 2006/24/CE, implicando a recolha massiva, indiscriminada de dados das comunicações e obrigando à sua conservação por um período compreendido entre seis meses e dois anos, o TJUE concluiu que «[u]ma regulamentação deste tipo não exige nenhuma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a segurança pública. Nomeadamente, não está limitada a uma conservação que tenha por objeto dados relativos a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de uma maneira ou de outra numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus

dados, podiam contribuir para a luta contra a criminalidade […]» (acórdão *Tele2*, n.º 106).

36.º

Tal significa que o TJUE considera ser contrária ao direito da União Europeia qualquer legislação nacional que preveja, para efeitos de luta contra a criminalidade, uma conservação *generalizada* e *indiferenciada* de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica, ou – dizendo o mesmo por outras palavras –, qualquer legislação nacional que obrigue os prestadores de serviços de comunicações eletrónicas a conservarem esses dados de forma sistemática, contínua e sem nenhuma exceção.

37.º

Entende o TJUE que tal sistema regulatório excede os limites do estritamente necessário e não pode ser considerado justificado, numa sociedade democrática, como exige o artigo 15.°, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta (cfr. acórdão *Tele2*, n.os 97-112).

38.º

Ora, na medida em que o sistema estabelecido pela Lei n.º 32/2008, de 17 de julho, pressupõe justamente, em lugar de uma conservação *selectiva* (cfr. acórdão *Tele2*, n.º 108), uma conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica, não há qualquer dúvida de que o regime estabelecido na lei nacional viola a Carta.

39.º

Além dessa desconformidade fundamental, relacionada com o próprio âmbito da obrigação de conservação de dados, a lei nacional é desconforme com as exigências decorrentes da jurisprudência do TJUE em matéria de *segurança e protecção dos dados conservados*.

40.º

Com efeito, a Lei n.º 32/2008, de 17 de julho, em nenhuma das alíneas do n.º 1 do artigo 7.º, estabelece especificamente o dever de os dados relativos às comunicações electrónicas serem conservados pelas operadoras de telecomunicações *no território da União Europeia* de modo a assegurar a efectividade da fiscalização (cfr. acórdão *Digital Rights Ireland*, n.º 68 e acórdão *Tele2*, n.os 122 e 125).

41.º

Por último, ao não estabelecer expressamente o dever de as autoridades competentes às quais tenha sido concedido o acesso aos dados desse facto informarem as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível de comprometer as investigações levadas a cabo por essas autoridades, a Lei n.º 32/2008, de 17 de julho, viola o direito da União Europeia (cfr. acórdão *Tele2*, n.os 121).

42.º

Estando a Lei n.º 32/2008 directamente vinculada pela Carta (artigo 51.º, n.º 1, da Carta), não pode o Tribunal Constitucional aplicar padrões nacionais de proteção dos direitos fundamentais que sejam susceptíveis de comprometer o nível de proteção previsto pela Carta, e, assim, o primado, a unidade e a efetividade do direito da União (acórdãos de 26 de fevereiro de 2013, *Melloni*, C-399/11, n.° 60 e *Åkerberg Fransson*, C-617/10, n.° 29).

43.º

De outra maneira, verificar-se-ia a situação anómala de, em virtude da interpretação dos direitos fundamentais à luz da Constituição da República Portuguesa, se permitir que na ordem jurídica nacional vigorem normas jurídicas contrárias à Carta dos Direitos Fundamentais da União Europeia.

44.º

Pelo que ainda que, no plano jurídico-constitucional, a declaração pelo TJUE da invalidade da Directiva 2006/24/CE não tenha como efeito automático a invalidade da Lei n.º 32/2008, a deliberação do Tribunal Constitucional quanto à conformidade das normas constantes desse acto legislativo com a Constituição da República Portuguesa deve adoptar uma fundamentação que, tanto quanto possível, seja consistente com a do TJUE nos acórdãos *Digital Rights Ireland* e *Tele2*.

45.º

Em virtude da directa vinculação à Carta da Lei n.º 32/2008, tal «dever de consistência na fundamentação» retira-se do *princípio da cooperação leal* a que a República Portuguesa – e, portanto, todos os órgãos do Estado, inclusive de índole jurisdicional – se encontra vinculada (artigo 4.º, n.º 3, do Tratado da União Europeia).

46.º

Em nosso entender, tanto bastaria para que o Tribunal Constitucional declarasse com força obrigatória geral, a inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, por violação do princípio da proporcionalidade na restrição dos direitos à

reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1) e por violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1).

47.º

Todavia, e independentemente da articulação entre a ordem jurídica nacional e a ordem jurídica europeia, os artigos 4.º, 6.º e 9.º da Lei n.º 32/2008 sempre se hão de considerar inconstitucionais à luz de parâmetros exclusivamente decorrentes do texto da Constituição da República.

B. Da violação do direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1)

1. *Da imposição legal de conservação de dados como agressão – e agressão* grave – *aos direitos fundamentais*

48.º

No acórdão n.º 403/2015, de 27 de Agosto, o Tribunal Constitucional, analisando a pertinente jurisprudência constitucional, reconhece que as circunstâncias em que as comunicações são realizadas integram o âmbito de protecção do direito à reserva da intimidade da vida

privada e familiar, consagrado no artigo 26.º, n.º 1, da Constituição (Ac. n.º 403/2015, AcTC, 93.º vol., 2015, pp. 45-101, pp. 60 e segs.).

49.º

Embora tal argumentação se dirija às questões de constitucionalidade relacionadas com o *acesso* pelas autoridades competentes a dados de tráfego e de localização, daí não deve retirar-se que a mesma não seja aplicável à própria imposição legal de conservação de dados. O Tribunal Constitucional apenas se não terá expressamente pronunciado sobre esta última dimensão do problema na exacta medida em que, atendendo ao objecto do pedido, tal como delimitado pelo requerente naquele processo, apenas se ocupou especificamente do regime de acesso aos dados, deixando de fora da sua análise o regime legal relativo à própria obrigação de conservação desses dados por parte das operadoras de telecomunicações.

50.º

O que é certo é que, argumentar-se que «[…] a manipulação ilegal ou ilegítima do conteúdo e das circunstâncias da comunicação pode violar a *privacidade* dos interlocutores intervenientes, atentando ou pondo em risco esferas nucleares das pessoas, das suas vidas, ou dimensões do seu modo de ser e estar [.] de sorte que a possibilidade de se aceder aos dados das comunicações colide com um conjunto de valores associados à *vida privada* que fundamentam e legitimam a proteção

jurídico-constitucional» (Ac. n.º 403/2015, AcTC, cit., p. 60), implica reconhecer que, independentemente do eventual acesso aos dados existentes, a mera imposição legal de conservação de dados integra o âmbito de protecção do direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1).

51.º

É isso que, em articulação com o acórdão n.º 128/92, conclui o Tribunal Constitucional: «De modo que, na jurisprudência constitucional, as *comunicações privadas*, englobando o *conteúdo* e *circunstancialismos* em que as mesmas têm lugar, são reconhecidas como um meio através do qual se manifestam aspetos da vida privada da pessoa e que, por isso, caem no âmbito da proteção constitucional da respetiva reserva (Ac. n.º 403/2015, AcTC, cit., p. 61).

52.º

Tal significa que, desde logo, a imposição às operadoras de comunicações electrónicas de conservação de dados de tráfego e de localização de todas as comunicações electrónicas consubstancia uma restrição – e uma restrição intensa ou grave – do direito à reserva da intimidade da vida privada e familiar, consagrado no artigo 26.º, n.º 1, da Constituição.

53.º

Na verdade, a mera existência de dados, agregados e guardados, por um período de um ano, em centros de conservação [em princípio] detidos e geridos pelas próprias empresas operadoras de telecomunicações, contendo informação extremamente sensível sobre a vida privada e familiar de milhões de cidadãos (*supra*, ponto 8), é um facto que gera por si só um permanente risco de violação da privacidade, ainda que tais dados nunca venham a ser acedidos, nos termos e para os efeitos legais, pelas autoridades para tal legitimadas.

54.º

Com efeito, por muito que se procure assegurar a sua inviolabilidade através da tecnologia a cada momento disponível, não é possível garantir em termos absolutos que não haja falhas de segurança, e que não ocorra o acesso ilegítimo, por parte de terceiros, a todo o manancial de informação que por este meio é conservado.

55.º

O problema assumirá ainda maior gravidade se se tiver em linha de conta que a autoridade pública competente para o controlo da aplicação das regras relativas à segurança e proteção de dados, a Comissão

Nacional de Protecção de Dados (artigo 7.º, n.º 3, da Lei n.º 32/2008) – autoridade à qual a lei, no seu artigo 14.º, conferiu a competência para a instrução dos processos de contraordenação e para a aplicação das correspondentes coimas –, decidiu, através da Deliberação n.º 1008/2017, de 18 de julho, «desaplicar [a Lei n.º 32/2008] nas situações que lhe sejam submetidas para apreciação», por entender que, sendo as normas nela inscritas lesivas, de acordo com o seu juízo, da Carta dos Direitos Fundamentais da União e da Constituição da República Portuguesa, deveria agir «em cumprimento do primado do Direito da União e da prevalência da Constituição» (*supra,* pontos 18 e 19). Assim, e face à ausência de fiscalização por parte da autoridade administrativa competente, podem agora os operadores de serviços de telecomunicações não dispor de qualquer desincentivo para incumprir as obrigações que sobre eles impendem, as quais deveriam corresponder às exigências de garantia de um «nível particularmente elevado de protecção e segurança».

56.º

O momento de agressão – e de agressão *grave* – aos direitos dá-se, portanto, logo com a obrigação, imposta às operadoras de telecomunicações, de conservação de todos estes dados. Não fora a previsão legal desta obrigação e jamais seria possível vir a verificar-se o acesso ilegítimo aos dados conservados por parte de terceiros, porquanto tais dados, pura e simplesmente, não existiriam.

57.º

A recondução da imposição legal de conservação de dados ao âmbito de protecção do artigo 26.º, n.º 1, é determinante no que respeita aos dados de localização fora do contexto de uma comunicação, se se partir do pressuposto segundo o qual não estarão tais dados cobertos pela garantia constitucional de sigilo das telecomunicações, consagrada no artigo 34.º, n.º 1 da CRP.

58.º

Ainda que se parta desse pressuposto – e se considere, como no caso do Acórdão n.º 486/2009, que relativamente a tal tipo de dados se estará sempre fora do âmbito de um *acto comunicacional concreto* – não poderá jamais esquecer-se a quantidade e qualidade da informação que por seu intermédio se poderá vir a obter: desde que a pessoa transporte consigo o seu telemóvel ou outro dispositivo electrónico de acesso à Internet, sempre será possível reconstituir aqueles que foram, ao longo do período de um ano, todos os lugares em que esteve, quanto tempo esteve em cada um desses lugares e, cruzando esta informação com dados respeitantes a outras pessoas, com quem esteve, onde e quando.

59.º

Embora seja predominante e generalizada a percepção segundo a qual a informação contida em dados de tráfego e de localização será menos invasiva da privacidade do que o conhecimento do próprio

conteúdo das comunicações, o que é certo é que se invoca a sua indispensabilidade para efeitos de investigação criminal.

60.º

Ora, se tais dados fossem inocentes e nada revelassem sobre a vida do indivíduo em causa, então seguramente que nenhum interesse haveria em recorrer a esses dados para efeitos de investigação criminal.

61.º

É precisamente por serem extremamente precisos na reconstituição da vida da pessoa em causa – de uma certa perspectiva, mais até do que o próprio conteúdo das comunicações efectuadas – que tais dados se revelam preciosos para as autoridades competentes na área da investigação criminal.

62.º

Assim, a imposição legal de conservação, por um período de um ano, de todos os «metadados», incluindo os dados de localização fora do contexto de uma comunicação, constitui, só por si, uma agressão séria e grave do direito à reserva da intimidade da vida privada e familiar, consagrado no artigo 26.º, n.º 1, da Constituição.

63.º

A questão que se põe é então a de saber se tal agressão, que, só por si, é séria e grave, se encontrará constitucionalmente justificada, o que implica que se analise a medida à luz das exigências decorrentes do princípio da proporcionalidade (artigo 18.º, n.º 2).

2. Da violação do princípio da proporcionalidade

64.º

Nos termos do disposto no artigo 3.º, n.º 1, da Lei n.º 32/2008, de 17 de julho, «a conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes». Nenhuma outra finalidade de interesse público é invocada pelo legislador como justificação para a medida que estabelece uma obrigação geral de conservação de dados.

65.º

Embora não haja qualquer informação de ordem *quantitativa* que nos dê a conhecer a dimensão exacta da realidade que, através da obrigação geral de conservação de dados, o legislador procurou combater, não restam dúvidas de que a [necessidade da] luta contra a criminalidade grave é, em si mesma, razão legítima de restrição de direitos fundamentais. Não apenas por ser tarefa fundamental do Estado a

garantia da paz e da segurança, esteio do exercício dos demais direitos e liberdades individuais e do respeito pelo Estado de direito democrático (artigos 9.º e 25.º); mas ainda por se mostrar especialmente adequado que os poderes públicos façam uso dos meios proporcionados pelo progresso tecnológico para levar a cabo a realização de tal tarefa estadual. Os dados de tráfego e de localização constituem pontos de referência em relação ao momento do crime, à localização de suspeitos na zona do crime ou nas suas proximidades, a comportamentos de suspeitos antes e depois do crime, às relações existentes entre os suspeitos, ao itinerário de fuga ou mesmo à indiciação de outros suspeitos. Que o acesso, por parte das autoridades públicas, a todo o acervo de informação que estes dados contêm seja uma medida adequada à prossecução das finalidades enunciadas na lei é pois algo que, *em abstracto*, não pode ser contestado.

66.º

Certo é, no entanto, que já existem na ordem jurídica medidas menos restritivas do que aquelas de que vimos falando – a conservação generalizada e indiferenciada durante todo um ano de todos os «metadados» respeitantes a todos os cidadãos – e que se mostram também elas adequadas à prossecução da finalidade que o n.º 1 do artigo 3.º da Lei n.º 32/2008 enuncia. É o que se verifica com o regime de preservação de dados (*quick freeze*), tal como previsto e regulado pelo artigo 12.º da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime, que transpõe 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).

67.º

Argumentar-se-á porventura, contra o que vimos dizendo, que a *eficácia* revelada pelo sistema do *quick freeze* no combate à criminalidade grave não é em si mesma equiparável àquela que é dispensada pelo sistema de conservação generalizada e indiferenciada de todos os «metadados». Nos seus próprios termos, o *quick freeze* é válido apenas para o caso concreto; e só é ordenado tendo como fundamento [concreto] a verificação de uma determinada suspeita. Em contrapartida, a obrigação geral de conservação de dados, ao permitir às autoridades públicas «a leitura do passado» de quem quer que seja, mostra-se operativa para além de qualquer suspeita que já se tenha, em certo caso concreto, formado. Dizendo de outro modo: enquanto a medida de «preservação de dados» [*quick freeze*] só é útil a partir do momento em que se tenha previamente identificado o suspeito da prática de um crime, a obrigação geral de conservação de dados será útil bem para além desse momento, na exacta medida em que ela própria *facilita* a identificação [dos suspeitos]. No combate à «criminalidade grave» não pode pois equiparar-se a eficácia revelada por um e outro sistema: a conservação generalizada e indiferenciada de dados é bem mais eficaz do que a mera «preservação» dos mesmos (Carlos Pinho, «Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?», *Revista do Ministério Público* 154, 2018, pp. 167-192, 179-185).

68.º

No entanto, o facto de certa medida legislativa se mostrar bem mais eficaz do que qualquer outra na realização de bens constitucionalmente protegidos não transforma tal medida em acção legítima, no quadro das restrições admissíveis a direitos e liberdades essenciais. Sendo este um postulado firme da dogmática dos direitos fundamentais, válido para qualquer acção do Estado, a sua aplicabilidade aos domínios da política criminal adquire reverberação especial: nem tudo o que se mostrar *especialmente eficaz* no combate à criminalidade grave será assim, e só em razão de tal eficácia, constitucionalmente justificado. Nesta medida, carecerá de reavaliação o argumento segundo o qual um sistema de conservação generalizada e indiferenciada de dados seria susceptível de superar o teste da necessidade (em que se analisa o princípio da proporcionalidade) por ser relativamente mais eficaz na luta contra a criminalidade do que um regime de preservação de dados (*quick freeze*).

69.º

Em uma ordem constitucional de liberdade, jamais pode todo e qualquer indivíduo que utilize um meio de comunicação ser tratado como um potencial criminoso em termos de ver sacrificado – e gravemente sacrificado – o seu direito fundamental à reserva da intimidade da vida privada e familiar.

70.º

É, no entanto, a necessidade desse mesmo sacrifício que o regime instituído pela Lei n.º 32/2008 assume, ao impor uma conservação generalizada e indiferenciada de todos os dados de tráfego e de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica. Uma obrigação geral de conservação de dados, ao não prever nenhuma diferenciação, limitação ou excepção em função do objectivo prosseguido – sendo inclusivamente aplicável a pessoas cujas comunicações estejam sujeitas a segredo profissional – afecta globalmente todas as pessoas que utilizem serviços de comunicações electrónicas, sem que essas pessoas se encontrem, ainda que indirectamente, em situação susceptível de justificar um procedimento criminal.

71.º

Assim, ao pressupor que todo e qualquer indivíduo deve ser, a título preventivo e de modo contínuo, *intensamente* vigiado, o regime instituído pela Lei n.º 32/2008 tem por efeito transformar em regra a conservação dos dados de tráfego e de localização. Todavia, de uma adequada aplicação do princípio da proporcionalidade não poderá deixar de retirar-se a ilação contrária. Sendo a intimidade da vida privada uma liberdade essencial, as restrições que os poderes públicos imponham a tal liberdade deverão ocorrer não por regra mas por excepção.

72.º

Tal natureza excepcional das restrições sempre poderia vir a ser garantida se o regime legal deixasse de ser absolutamente *indeterminado* quanto às circunstâncias e às condições em que é legítimo proceder à conservação dos dados – limitando, por hipótese, tal conservação a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que pudessem estar envolvidas de uma maneira ou de outra na prática de infrações graves – e definisse um período mais curto (não de um ano) para a manutenção da obrigação.

73.º

A este propósito, importa observar que o Tribunal Constitucional Federal alemão, na decisão de 2 de Março de 2010, que declarou a inconstitucionalidade das alterações introduzidas à *Telekommunikationsgesetz* e à *Strafprozessordnung* pela lei que transpusera a Directiva 2006/24/CE, embora tenha considerado que o prazo nela previsto para a conservação de dados, seis meses, não violava os direitos fundamentais, não deixou de observar que se estava já muito próximo daquilo que, de acordo com as exigências decorrentes do princípio da proporcionalidade, seria o limite máximo constitucionalmente admissível.

74.º

Elucidativo é ainda o facto de, na sequência dessa decisão, o legislador alemão ter, em 2015, voltado a aprovar uma lei a impor às operadoras de telecomunicações a conservação de dados – até então e desde 2010, com a declaração de inconstitucionalidade das alterações introduzidas à *Telekommunikationsgesetz* e à *Strafprozessordnung* pela lei que transpusera a Directiva 2006/24/CE, não havia enquadramento legal nesta matéria –, reduzindo substancialmente os limites máximos da duração da conservação de dados. Agora, na República Federal da Alemanha, e em virtude da aprovação da *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*, de 10 de Dezembro de 2015, (BGBl. I S. 2218 ff.), foram introduzidas alterações à *Telekommunikationsgesetz*, de 22 de Junho de 2004, (BGBl. I S. 1190), prevendo-se no § 113b desta última um prazo máximo de conservação de 10 semanas no que respeita a dados de tráfego e um prazo máximo de conservação de 4 semanas no que se refere a dados de localização[2].

75.º

De acordo com as motivações expressas pelo legislador, este regime procuraria responder à necessidade de *dispersar*, ou de pelo menos evitar uma *excessiva concentração*, [d]os dados conservados. Ao limitar a quatro semanas o período de conservação dos dados de localização, a lei alemã não só se mostra particularmente sensível à qualidade e delicadeza da informação que este tipo de dados transmite,

[2] Aparentemente, a aplicação deste novo regime encontrar-se-á neste momento suspensa, em virtude da abertura de novos processos judiciais contestando ainda a validade de algumas das suas normas.

como procura ainda impedir que, para além desse período, se possa concentrar toda essa informação através do «cruzamento» dos dados de tráfego com os dados de localização, com a consequente largueza de conhecimentos – e, logo, de possibilidade de reconstituição do passado de cada um – que tal «cruzamento» faculta.

76.º

Em Portugal, a imposição legal de conservação de dados, com a amplitude, duração e indiferenciação que decorre dos artigos 4.º e 6.º, da Lei n.º 32/2008, de 17 de julho, ao aplicar a mesma disciplina jurídica a qualquer que seja a categoria de dados em causa e ao impor a conservação dos dados por um período indevidamente longo, traduz uma restrição excessiva do direito individual à privacidade. Mas comporta, do mesmo passo, o risco de lesão efectiva de outros direitos e liberdades, constitucionalmente consagrados.

77.º

Com efeito, a conservação de tamanha amplitude de dados respeitantes às circunstâncias de todas as comunicações efectuadas por todos os cidadãos (destinatários [pertença a determinadas categorias profissionais, instituições, associações ou grupos de representação de interesses], data, hora e localização das chamadas telefónicas), permite, ao combinar e cruzar esses dados, inferir, com precisão, informações detalhadas sobre padrões de vida individuais, círculos sociais de pertença,

inclinações político-partidárias, bem como aspectos da vida pessoal, tais como rotinas, hobbies, vulnerabilidades (por exemplo, em matéria de saúde). Além da agressão que tal constitui para cada indivíduo, enquanto titular de um direito básico à reserva da privacidade, do acesso ilegítimo de terceiros a todo este manancial de informação podem resultar constrições graves ao exercício de outros direitos e liberdades, nomeadamente os que se encontram consagrados no Capítulo II do Título II da Parte Primeira da Constituição da República.

C. Da violação do sigilo das comunicações (artigo 34.º, n.º 1)

78.º

O artigo 34.º, n.º 1, consagra o sigilo das comunicações, o qual protege contra o conhecimento por parte do poder público a transmissão, com a ajuda dos meios de comunicação disponíveis, de informação a receptores individuais.

79.º

O sigilo das comunicações abrange não apenas o conteúdo do que é transmitido entre o emissor e o receptor mas também as circunstâncias

da comunicação, designadamente se, quando, com que frequência, através de que meio de comunicação e entre quem é que são estabelecidas comunicações.

80.º

O Tribunal Constitucional, chamado a pronunciar-se sobre a questão, não teve qualquer dúvida em considerar que «[...] a proibição de ingerência nas comunicações, constante do artigo 34.º da CRP, abrange os dados de tráfego» (Ac. n.º 403/2015, cit., p. 65).

81.º

Uma vez mais, importa aqui observar que, embora tal argumentação seja feita a propósito do *acesso* pelo Estado a dados de tráfego e de localização, daí se não deve retirar que o mesmo não seja aplicável à própria imposição legal de conservação de dados. O Tribunal Constitucional apenas se não terá expressamente pronunciado sobre essa dimensão do problema na exacta medida em que, atendendo ao objecto do pedido, tal como delimitado pelo requerente nesse processo, apenas se ocupou especificamente do regime de acesso aos dados, deixando de fora da sua análise o regime legal relativo à própria imposição legal de conservação de dados às operadoras de telecomunicações.

82.º

Aliás, a construção dogmática elaborada nesse aresto e que serve de suporte à construção do direito à autodeterminação comunicativa, nos termos do qual o mesmo se analisa «[...] em uma dupla vertente, enquanto proteção de uma reserva da vida privada e enquanto liberdade de atuação, ou seja, uma conexão entre "segredo das comunicações" e "liberdade de comunicação"» (Ac. n.º 403/2015, AcTC, cit., p. 63), densifica a protecção constitucional, tornando claro que as questões de constitucionalidade relativas ao *acesso*, de que especificamente se ocupa o n.º 4 do artigo 34.º, são apenas uma das múltiplas dimensões da protecção constitucional globalmente conferida por esse preceito constitucional.

83.º

A protecção que a Constituição confere respeita não apenas ao momento de acesso por parte das autoridades públicas, mas a cada acto do poder público susceptível de afectar o sigilo das telecomunicações.

84.º

O acto do legislador consistente em impor às operadoras de telecomunicações, por um período de um ano, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de

localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica, consubstancia, em si mesmo considerado – e independentemente das disposições que visam regular o seu posterior eventual acesso por parte das autoridades –, uma agressão – e uma agressão *grave* – por parte do Estado ao sigilo das comunicações, constitucionalmente garantido no artigo 34.º, n.º 1.

85.º

No mesmo sentido concluiu o Tribunal Constitucional Federal alemão na já referida decisão de 2 de Março de 2010, a respeito da disposição da Lei Fundamental alemã que, em termos equivalentes ao artigo 34.º, n.º 1, da Constituição portuguesa, consagra o sigilo das comunicações.

86.º

A questão que se põe é, uma vez mais, a de saber se tal agressão, que, só por si, é séria e grave, será constitucionalmente justificada, o que implica que se analise a medida à luz das exigências decorrentes do princípio da proporcionalidade (artigo 18.º, n.º 2).

87.º

Nestes termos, serão também aqui aplicáveis as considerações feitas a propósito da desproporcionalidade da restrição do direito à reserva da intimidade da vida privada (*supra*, pontos 64-77).

88.º

Isto é assim, desde logo, em virtude da dupla vertente do direito à autodeterminação comunicativa, considerando que entre os diferentes bens-jurídico constitucionais através deste direito protegidos se encontra a reserva da intimidade da vida privada (Ac. n.º 403/2015, cit., p. 62).

89.º

Mas também no que respeita à outra vertente do direito à autodeterminação comunicativa, centrada no domínio de actuação do indivíduo – liberdade para comunicar e liberdade para desenvolvimento das relações interpessoais – não deixam de valer as considerações anteriormente expendidas.

90.º

Por muito elevado que seja o peso a atribuir à razão de interesse público que sustenta a medida de conservação de dados – uma maior eficácia na luta contra a criminalidade grave –, tal peso não justifica a intensidade do sacrifício imposto ao direito ao sigilo das comunicações: o indivíduo viver com a sensação de estar a ser permanentemente vigiado e, por causa disso, retrair-se e inibir-se na comunicação com as outras

pessoas para não deixar rasto do exercício de liberdades que a Constituição tem como fundamentais.

91.º

Pelo que deve entender-se que a imposição legal de conservação de dados, com a amplitude, duração e indiferenciação que decorrem dos artigos 4.º e 6.º, da Lei n.º 32/2008, de 17 de julho, ao aplicar a mesma disciplina jurídica a qualquer que seja a categoria de dados em causa e ao impor a conservação dos dados por um período indevidamente longo, constitui uma restrição desproporcionada do sigilo das telecomunicações, consagrado no artigo 34.º, n.º 1, da Constituição.

D. Da violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1)

92.º

A Lei n.º 32/2008, de 17 de julho, não prevê que as autoridades nacionais competentes às quais é concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos aplicáveis.

93.º

Esse dever de comunicação ao interessado não está assegurado em nenhum outro lugar da ordem jurídica (não sendo nomeadamente previsto pelo Código de Processo Penal).

94.º

Não se vê, porém, como pode vir a ser cumprido o princípio constitucional da tutela jurisdicional efectiva, constante do artigo 20.º da Constituição da República, sem a consagração legal deste dever de comunicação. O artigo 9.º da Lei nº 32/2008 define o procedimento que deve ser seguido para que os dados conservados pelas operadoras possam ser transmitidos às autoridades competentes. Todavia, o facto de se não prever, em momento algum desse procedimento, a necessidade de informar o interessado (a pessoa a que se referem os dados que foram transmitidos) quanto à existência mesma do procedimento, faz com que tal existência se torne imperceptível aos olhos de quem por ela é afectado. Nestas circunstâncias, comprometidas ficam, não apenas a possibilidade de se vir a conhecer a informação que, a respeito de cada um, obteve a autoridade pública, mas ainda a faculdade de reacção e defesa contra eventuais acessos ilegítimos a essa mesma informação.

95.º

Porque assim é, a circunstância de, nos termos do disposto no artigo 9.º, da Lei n.º 32/2008, de 17 de julho, o eventual acesso aos dados por parte das autoridades competentes ser precedido de autorização judicial por parte do juiz de instrução em nada altera os dados da questão; como em nada os altera a circunstância de a comunicação poder vir a comprometer as investigações levadas a cabo pelas autoridades competentes. Para que o procedimento previsto no artigo 9.º da Lei n.º 32/2008 se mostre inteiramente conforme com o disposto no artigo 20.º da CRP necessário é que a comunicação à pessoa afectada se faça, ainda que tal ocorra apenas *a partir do momento em que a mesma* [comunicação] *não seja já susceptível de comprometer as investigações* (*supra*, ponto 41).

96.º

Neste contexto, configurar-se-á ainda admissível a decisão de não-comunicação, naqueles casos em que for manifesto que de qualquer informação prestada ao interessado – independentemente do momento em que ocorra – sempre resultará a frustração da investigação ou perigo para vida ou integridade física de terceiros. Todavia, em tais circunstâncias, a conformidade do regime legal com as exigências constitucionais que vimos mencionando exigirá que a decisão de não-comunicação, além de fundamentada, seja judicialmente validada.

97.º

Todavia, o regime instituído pela Lei nº 32/2008 é todo ele silente quanto a este dever de comunicação, seja ele cumprido em que momento for e tenha ele as excepções que tiver.

98.º

Tal confere, em nosso entender, um argumento adicional para a declaração de inconstitucionalidade do disposto nos artigos 4.º e 6.º da referida lei. A imposição legal de conservação de dados que nestes artigos se prevê, para além de infringir, pela sua amplitude, duração e indiferenciação, as normas constitucionais relativas à reserva de privacidade e ao sigilo das comunicações, não permite que o interessado tenha qualquer controlo sobre o destino dos dados que são conservados, assim se excluindo a possibilidade de defesa perante um eventual acesso ilegítimo. Nestes termos, também por este motivo será inconstitucional o regime decorrente dos artigos 4.º e 6.º da Lei n.º 32/2008.

99.º

No entanto, constitui por si só uma violação do disposto no artigo 20.º, n.º 1, da Constituição da República o facto de o artigo 9.º da Lei n.º 32/2008 em momento algum prever a necessária comunicação aos interessados, sempre que os dados conservados sejam, nas condições aí definidas, transmitidos às autoridades competentes. A ausência, do conteúdo prescritivo deste artigo 9.º, de uma qualquer disciplina jurídica

que garanta – quiçá através da previsão de um procedimento próprio – que as pessoas possam exercer o seu direito a uma tutela juridcional efectiva contra acessos ilegítimos por parte das autoridades aos dados conservados, torna, em nosso entender, todo o regime naquele artigo instituído contrário à ordem constitucional portuguesa.

Nestes termos, requer-se ao Tribunal Constitucional que aprecie e declare, com força obrigatória geral:

(i) a inconstitucionalidade, por violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1) e ao sigilo das comunicações (artigo 34.º, n.º 1) e por violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1), do disposto nos artigos 4.º e 6.º, da Lei n.º 32/2008, de 17 de julho;

(ii) a inconstitucionalidade, por violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1), do disposto no artigo 9.º da Lei n.º 32/2008, de 17 de julho.

A Provedora de Justiça,

(*Maria Lúcia Amaral*)

Lisboa, 26 de agosto de 2019