COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

DELIBERAÇÃO N.º 641/2017

I. Justificação da deliberação

O Tribunal de Justiça da União Europeia (TJUE) declarou a invalidade da Diretiva 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, que altera a Diretiva 2002/58/CE. A declaração foi proferida no acórdão *Digital Rights Ireland, Ltd.,* de 8 de abril de 2014, no âmbito de reenvios prejudiciais que deram origem aos processos C-293/12 e C-594/12[1].

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

Sendo certo que a declaração de invalidade da Diretiva não implica diretamente a invalidade da lei nacional que a transponha, é igualmente certo que a Carta vincula os Estados-Membros, por força do Tratado sobre a União Europeia, tendo por isso aqueles de respeitar os direitos e observar os princípios nela consagrados (cf. n.º 1 do artigo 51.º). Nessa medida, do juízo de desconformidade, em relação à Carta, do regime europeu de retenção de dados de comunicações eletrónicas não pode deixar de decorrer um dever para os Estados Membros de reavaliar a conformidade com a Carta dos respetivos regimes nacionais de retenção de dados produzidos em transposição daquela diretiva, à luz dos fundamentos expostos no acórdão do TJUE.

Para a necessidade da reavaliação da Lei n.º 32/2008, de 17 de julho, que transpôs a Diretiva n.º 2006/24/CE para a ordem jurídica portuguesa, em termos de conformidade chamou a Comissão Nacional de Protecção de Dados (CNPD) a atenção da Assembleia da República (em 29 de abril de 2014, por ocasião da audição na Comissão dos Assuntos Constitucionais,

[1] Disponível em http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d63d34ffbab785491ab755b34740570fe7.e34KaxiLc3eQc40LaxqMbN4Pax0Qe0?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=48371.

Direitos, Liberdades e Garantias), tendo ainda sublinhado no Parecer n.º 51/2015 a necessidade de análise da validade de tal diploma legal e, recentemente e de modo mais incisivo, no Parecer n.º 24/2017, assinalando a desconformidade da Lei n.º 32/2008 em relação ao Direito da União Europeia, maxime à Carta, bem como em relação à Constituição da República Portuguesa (CRP).

Entretanto, em 21 de dezembro de 2016, o TJUE, no acórdão *Tele2* (processos n.º C-203/15 e C-698/15)[2], voltou a pronunciar-se sobre esta matéria, agora a propósito dos regimes legais de dois Estados-Membros da União Europeia que transpuseram aquela Diretiva[3].

Neste acórdão, partindo da invalidade da Diretiva 2006/24/CE, o Tribunal entendeu que os Estados membros estão ainda vinculados pela Carta na definição de regimes legais de retenção de dados de comunicações eletrónicas, por se tratar de um poder que é reconhecido e delimitado pelo artigo 15.º, n.º 1, 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 (Diretiva relativa à privacidade e às comunicações eletrónicas), alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (cf. §§ 64 e 71-81 do acórdão *Tele2*). Recorda-se que, como a Diretiva 2006/24 foi declarada inválida, o Tribunal não aplica o n.º 1-A do artigo 15.º da Diretiva 2002/58, que precisamente ressalvava o regime jurídico europeu da retenção de dados.

Assim, a pronúncia do Tribunal incide sobre a conformidade das regras nacionais de retenção de dados por referência ao disposto no n.º 1 do artigo 15.º da Diretiva 2002/58, que se transcreve:

«Os Estados-Membros podem adoptar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1 a 4 do artigo 8.º e no artigo 9.º da presente directiva sempre que essas restrições constituam uma medida necessária,

---

[2] Disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=48416.

[3] Em causa está a legislação nacional da Suécia e do Reino Unido que transpunha a Diretiva 2006/24/CE, implicando a recolha massiva, indiscriminada de dados das comunicações e obrigando à sua conservação por um período compreendido entre 6 meses e dois anos (tal como previsto nos seus artigos 5.º e 6.º daquela Diretiva).

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas, tal como referido no n.º 1 do artigo 13.º da Directiva 95/46/CE.

Para o efeito, os Estados-Membros podem designadamente adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.ºs 1 e 2 do artigo 6.º do Tratado da União Europeia».

Distinguindo as duas operações sobre dados pessoais – a conservação e o acesso – o TJUE concluiu que o *artigo 15.°, n.° 1, da Diretiva 2002/58/CE [...] lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, 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 eletrónica* (cf. §112).

E, quanto ao acesso, considerou que o mesmo artigo *deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula [...] o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União* (cf. § 125).

Sublinhou ainda o TJUE que é dever dos Estados Membros, mais especificamente dos órgãos jurisdicionais, *verificar se e em que medida as regulamentações nacionais [...] respeitam as exigências que decorrem do artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, tanto no que se refere ao acesso das autoridades nacionais competentes aos dados conservados como à proteção e ao nível de segurança desses dados.*

Em face da jurisprudência do TJUE, entende a CNPD ser seu dever alertar a Assembleia da República para a necessidade de reavaliar a Lei n.º 32/2008, de 17 de julho, em termos de conformidade com a Carta, mas também com a CRP, já que os direitos fundamentais restringidos por aquele regime têm consagração constitucional e a restrição legal de tais direitos obedece nos termos constitucionais ao mesmo princípio da proporcionalidade.

Assim, no exercício da competência definida no n.º 4 (parte final) do artigo 22.º e no n.º 4 do artigo 23.º da LPDP, vem a CNPD recomendar a revisão da Lei n.º 32/2008, de 17 de julho, para garantia dos direitos fundamentais à reserva da intimidade da vida privada, à inviolabilidade das comunicações e à proteção dos dados pessoais, passando a explicitar a sua perspetiva.

II. A Lei n.º 32/2008 e os tratamentos de dados pessoais

1. Descrição sumária do regime legal

Recorda-se que nos termos da Lei n.º 32/2008, as operadoras de comunicações eletrónicas têm o dever de conservar pelo período de um ano os dados de tráfego e de localização de todas as comunicações eletrónicas, os quais vêm especificados no artigo 4.º do mesmo diploma.

Não restando dúvidas de que os dados de tráfego e de localização são dados pessoais, no sentido da alínea a) do artigo 3.º da LPDP[4], por revelarem aspetos da vida privada dos seus titulares, os mesmos integram a categoria de dados sensíveis, estando especialmente protegidos pela CRP (cf. n.º 4 do artigo 34.º e n.º 3 do artigo 35.º) e pela lei (cf. n.ºs 1 e 2 do artigo 7.º da LPDP). Com efeito, em causa estão dados que revelam a todo o momento aspetos da vida privada e familiar dos indivíduos: permitindo rastrear a localização do cidadão ao longo do dia, todos os dias (desde que transporte o telemóvel ou outro dispositivo eletrónico de acesso à Internet), e identificar com quem contacta (chamada – inclusive as tentadas e não concretizadas – por telefone ou telemóvel, envio ou receção de SMS, MMS, ou de correio

[4] Entendimento já acolhido pelo TJUE, no Acórdão *Digital Rights Ireland Ltd.* e no Acórdão *Tele 2.*

eletrónico), bem como a duração e a regularidade dessas comunicações e os sítios da Internet consultados[5].

A tais dados, dispõe essa lei, só podem aceder as autoridades judiciárias e as autoridades de polícia criminal elencadas na alínea f) do n.º 1 do artigo 2.º deste diploma legal e para a finalidade de investigação, deteção, repressão de crimes graves por parte destas autoridades, mediante autorização fundamentada do juiz. A Lei especifica ainda que os dados só podem dizer respeito a suspeito ou arguido, a pessoa que sirva de intermediário e a vítima de crime.

Começa-se por destacar que a Lei n.º 32/2008, ao contrário da Diretiva, especifica os crimes cuja prevenção, deteção e repressão justifica a imposição deste tratamento de dados pessoais (cf. alínea g) do n.º 1 do artigo 2.º), e sujeita ainda a controlo judicial prévio o acesso aos dados pelas autoridades competentes (cf. alínea a) do n.º 1 do artigo 7.º).

Mas se se pode reconhecer que as regras aqui definidas quanto ao acesso às bases de dados das comunicações eletrónicas oferecem, em parte, garantias adequadas a atenuar o impacto que tal tratamento de dados tem sobre a privacidade das pessoas, já o mesmo não pode afirmar-se quanto ao tratamento de dados pressuposto por aquele acesso e que é também definido na lei: a retenção ou conservação dos dados pessoais relativos às comunicações.

A exposição subsequente incidirá, primeiramente, no regime de conservação dos dados, para só depois se centrar no regime de acesso aos dados conservados.

2. O regime de conservação dos dados pessoais

O TJUE reconheceu que as medidas previstas na Diretiva, e que grosso modo correspondem à imposição do dever de conservação de dados de tráfego e de localização gerados no contexto de comunicações eletrónicas e do dever da sua transmissão a autoridades competentes para a finalidade de investigação, deteção e repressão de crimes graves, são

[5] Note-se que o n.º 4 do artigo 34.º da CRP, quando se refere a *toda* a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, pretende com isso proibir não apenas o conhecimento do *conteúdo* das comunicações mas também todas *as informações associadas aos meios de comunicação*: os chamados dados de tráfego e de localização (neste sentido, J. J. Gomes Canotilho/ Vital Moreira, *Constituição da República Portuguesa Anotada*, I, Coimbra Editora 2007, anot. VIII ao artigo 34.º, p. 544; Germano Marques da Silva/ Fernando Sá, in Jorge Miranda/ Rui Medeiros, *Constituição Portuguesa Anotada*, I, 2.ª ed., Coimbra Editora, anotações XIV e XVI ao artigo 34.º, p. 772-774).

legítimas e adequadas ao fim visado. Mas, quanto à necessidade de tais medidas, concluiu pela violação do princípio da proporcionalidade nessa vertente.

O principal argumento em que assenta tal juízo prende-se com o facto de a conservação dos dados constituir uma restrição aos direitos fundamentais à vida privada e à proteção de dados pessoais (cf. §§26-27, 31, 33-34 do acórdão *Digital Rights Ireland, Ltd.,* e §§ 98-100 do acórdão *Tele2),* não se excluindo a sua incidência no exercício da liberdade de expressão (cf. §28 do acórdão *Digital Rights Ireland, Ltd.,* e § 101 do acórdão *Tele2*), e que afeta a totalidade da população. Ou seja, o tratamento de dados pessoais e consequente restrição daqueles direitos fundamentais *abrange de maneira geral todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego* [...] (§57 do acórdão *Digital Rights Ireland, Ltd.,* cf. também § 103 do acórdão *Tele2*), aplicando-se mesmo a *pessoas em relação às quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com infrações graves* (§ 58 do acórdão *Digital Rights Ireland, Ltd.,* e § 105 do acórdão *Tele2*), traduzindo-se tal conservação num tratamento automático de dados pessoais com risco significativo de abuso e de acesso ilícito aos mesmos.

E neste ponto, isto é, no que diz respeito ao tratamento principalmente regulado na Lei n.º 32/2008, que é o da retenção dos dados pessoais, em que assenta a restante regulação legal, a lei nacional padece do mesmo vício que a Diretiva.

a. *Desproporcionalidade do regime de retenção dos dados*

Com efeito, o dever de conservação dos dados imposto às operadoras dos serviços de comunicação eletrónica respeita a todos os dados de tráfego e de localização de todos os clientes ou utilizadores das comunicações eletrónicas no território nacional. Sem que se atenda a um específico indício que permita associar uma pessoa a um concreto crime, mesmo que apenas como suspeito.

Acresce que não se excecionam deste dever de conservação os dados de tráfego e de localização daqueles que, nos termos de outros diplomas legais, estão vinculados e protegidos pelo segredo profissional (cf. §58 do acórdão *Digital Rights Ireland, Ltd.,* e § 105 do acórdão *Tele2*).

Como sublinha o TJUE no acórdão *Tele2, embora a eficácia da luta contra a criminalidade grave, nomeadamente contra a criminalidade organizada e o terrorismo, possa depender em larga medida da utilização de técnicas modernas de investigação, um objetivo de interesse geral desse tipo, por muito fundamental que seja, não pode por si só justificar que uma regulamentação nacional que prevê a conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização seja considerada necessária para efeitos da referida luta* (§ 103; cf. ainda § 51 do acórdão *Digital Rights Ireland, Ltd.*).

E salienta que *uma regulamentação deste tipo tem por efeito [...] que a conservação dos dados de tráfego e dos dados de localização constitui a regra, ao passo que o sistema implementado pela Diretiva 2002/58 exige que essa conservação dos dados seja a exceção* (§104). Na verdade, a possibilidade que é reconhecida no n.º 1 do artigo 15.º da Diretiva 2002/58 afigura-se como um desvio ou exceção ao regime estatuído ao longo desse diploma, essencialmente garantístico da proteção da privacidade no âmbito das comunicações eletrónicas.

Prevendo a Lei n.º 32/2008 um tratamento de dados pessoais automático, relativo aos dados de *todos* os clientes ou utilizadores de comunicações eletrónicas, que não permite uma seleção dos dados sujeitos a conservação em função da ligação do seu titular, ainda que indireta, a crimes graves, nem permite excluir dessa conservação dados das pessoas que, legalmente, não podem ser objeto de controlo por estarem abrangidos pelo sigilo profissional, forçoso é concluir-se pela invalidade da mesma por violação do princípio da proporcionalidade na restrição dos direitos ao respeito pela vida privada e familiar e pelas suas comunicações e à proteção dos dados pessoais, previstos nos artigos 7.º e 8.º da Carta e, paralelamente, no n.º 1 do artigo 26.º e nos n.ºs 1 e 3 do artigo 35.º, bem como no n.º 4 do artigo 34.º da CRP.

b. Outros aspetos do regime de retenção dos dados

Para além deste juízo geral de desnecessidade do tratamento de dados tal como se encontra previsto e imposto, a Lei n.º 32/2008 está também quanto a outros aspetos específicos em contradição com o Direito da União Europeia.

No que às medidas de segurança diz respeito, o mesmo artigo 7.º limita-se a repetir, com algumas adaptações, o disposto no artigo 7.º da Diretiva, sem especificar regras quanto às

medidas de segurança, nem as adaptar à quantidade, sensibilidade e especial risco de abuso e de acesso ilícito (cf. §66 do acórdão *Digital Rights Ireland, Ltd.*, e §122 do acórdão *Tele2*).

Além disso, incorrendo no mesmo vício que foi assinalado pelo TJUE à Diretiva, a Lei não impõe que os dados sejam conservados dentro do território da União, não estando assim garantida a fiscalização por entidades independentes como determina o n.º 3 do artigo 8.º da Carta (cf. §68 do acórdão *Digital Rights Ireland, Ltd.*, e §§122 e 123 do acórdão *Tele2*).

Em relação ao prazo de conservação dos dados pessoais, embora a Lei, no seu artigo 6.º, preveja um prazo mais curto do que o máximo admitido pela Diretiva, não se explicita qualquer elemento que permita compreender a razão de ser do prazo de um ano legalmente fixado – não sendo a opção legislativa neste ponto livre, por também estar sujeita ao princípio da proporcionalidade, sobram dúvidas quanto à observância do mesmo. E, considerando o tipo de crimes em causa, é questionável que o conhecimento do crime não implique o imediato acesso aos dados[6]; pelo que a regra há de ser a de um período de conservação mais curto para a generalidade dos dados de tráfego e dos dados de localização.

Em todos estas normas denota-se a ausência de especificação legal dos termos e condições em que pode ser realizado o tratamento de dados imposto, de modo a restringi-lo ao estritamente necessário à prossecução da respetiva finalidade, em violação do princípio da proporcionalidade.

3. O regime de acesso às bases de dados

No que ao regime de acesso às bases de dados diz respeito, a Lei n.º 32/2008 apresenta, como se disse supra, garantias que atenuam o impacto que este tratamento de dados pode ter na esfera jurídica dos cidadãos, assegurando a tutela dos seus direitos fundamentais.

Por um lado, limita o acesso às autoridades judiciárias e as autoridades de polícia criminal elencadas na alínea f) do n.º 1 do artigo 2.º deste diploma legal e para a finalidade de investigação, deteção, repressão de crimes graves por parte destas autoridades, sendo que os dados podem dizer respeito a suspeito ou arguido, a pessoa que sirva de intermediário e a

---

[6] Ou, ao abrigo da Lei do Cibercrime, a emissão em curto prazo de tempo de ordem de conservação dos dados no âmbito do correspondente processo.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

vítima de crime. Por outro lado, sujeita a autorização judicial prévia o acesso aos dados pelas autoridades competentes (cf. alínea a) do n.º 1 do artigo 7.º).

Não obstante, o regime legal cria ainda risco de abuso no acesso aos dados, ao omitir, tal como a Diretiva, critérios objetivos que permitam definir o perfil e limitar, ao estritamente necessário, o número das pessoas com autorização de acesso e de utilização posterior dos dados conservados (cf. §62 do acórdão *Digital Rights Ireland, Ltd.*). Na verdade, a alínea d) do n.º 1 do artigo 7.º da Lei n.º 32/2008 não apresenta critérios que densifiquem o conceito de «pessoas especialmente autorizadas», limitando-se a repetir a fórmula consagrada na Diretiva e que foi objeto de censura pelo TJUE[7].

III. Conclusões

1. Com os fundamentos expostos e que seguem de perto a jurisprudência do Tribunal de Justiça da União Europeia, a CNPD entende que a Lei n.º 32/2008 contém normas que preveem a restrição ou ingerência nos direitos fundamentais ao respeito pela vida privada e pelas comunicações e à proteção dos dados pessoais com grande amplitude e intensidade, em clara violação do princípio da proporcionalidade e, portanto, em violação do n.º 1 do artigo 52.º da Carta dos Direitos Fundamentais da União.
   Com os mesmos fundamentos, verifica-se uma restrição desproporcionada dos direitos à reserva da intimidade da vida privada, à inviolabilidade das comunicações e à proteção de dados pessoais, em violação do disposto no n.º 2 do artigo 18.º da Constituição da República Portuguesa.

   Recomenda, por isso, a CNPD a revisão da Lei n.º 32/2008, de 17 de julho.

---

[7] A este propósito, refira-se que o n.º 3 do artigo 7.º da Lei n.º 32/2008, que prevê a regulamentação do meio de comunicação eletrónica destes dados pessoais sensíveis, impondo a adoção de medidas técnicas que garantam a elevada proteção dos dados e a elevada segurança das comunicações, se concretizou na Portaria 469/2009, de 6 de maio, alterada por último pela Portaria n.º 694/2010, de 16 de agosto. Aí se determina que a utilização do sistema de comunicação criado é de utilização facultativa até que seja emitido despacho conjunto dos membros do Governo responsáveis pelas áreas da administração interna e da justiça a impor a obrigatoriedade da sua utilização.
Ora, até à presente data, apesar dos investimentos feitos por parte das operadoras de comunicações eletrónicas e por parte do Estado, o sistema de comunicação criado não é utilizado, com evidente prejuízo para a segurança das comunicações e para a proteção dos dados pessoais, que o artigo 7.º visava garantir.

2. Ainda em conformidade com a jurisprudência daquele Tribunal, a CNPD esclarece que, em face do estatuído no n.º 1 do artigo 15.º da Diretiva 2002/58, o legislador nacional pode definir um novo quadro jurídico de retenção de dados pessoais no âmbito das comunicações eletrónicas que permita, a título preventivo, a *conservação seletiva* dos dados de tráfego e dos dados de localização, o qual, todavia, tem, como impõe esta Diretiva e decorre da Constituição e da Carta, de respeitar o princípio da proporcionalidade (cf. §108 do acórdão *Tele2*).

   Assim, como estabelece o TJUE, a lei deve definir critérios objetivos de retenção dos dados *que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, de contribuir para a luta contra a criminalidade grave ou de prevenir um risco grave para a segurança pública* (cf. §111 do acórdão *Tele2*).

   Nesse sentido, o regime deve distinguir as situações de uma concreta suspeita de prática de crime grave das situações em que haja indícios fortes de preparação de crimes graves.

   Na primeira hipótese, a preservação dos dados pode ser feita quanto a uma ou mais pessoas direta ou indiretamente relacionadas com a concreta atividade criminosa e ainda assim restrita às categorias de dados adequadas e necessárias à investigação (reconhecendo-se ao juiz o poder de definir os dados relevantes no caso concreto); na hipótese de risco elevado de preparação ou de execução desses atos criminosos, detetada pelas autoridades competentes com base em elementos objetivos, deve a recolha e conservação dos dados ser determinada por forma a não ser ilimitada, designadamente, como sugere o TJUE, em função de um critério geográfico e por um período de tempo previamente definido[8].

Lisboa, 9 de maio de 2017

Filipa Calvão (Presidente)

---

[8] Uma delimitação normativa deste tipo permitiria, por exemplo, a conservação de todos os dados de tráfego e dos dados de localização na área geográfica de Fátima por ocasião da visita papal ou de outros eventos que apresentem um elevado risco concreto.