Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental

The Directive 2006/24 declaration of invalidity and the consequences of metadata retention in the EU Member States: A Fundamental Rights Standards Approach

Submitted: 15/01/2017
Revised: 12/02/2017
Accepted: 07/03/2017

Alessandra Silveira[*]
Pedro Miguel Freitas[**]

Resumo

Propósito: O texto se ocupa da recente jurisprudência do Tribunal de Justiça da União Europeia (TJUE) sobre a conservação de dados ("metadados") por fornecedores de serviços de comunicações eletrónicas para efeitos de investigação, deteção e repressão de infrações graves. Os autores procuram deslindar as implicações, para as autoridades dos Estados-Membros da União Europeia (UE), da declaração de invalidade da diretiva que regulava a matéria, por forma a afastar uma diferenciação ilegítima de tratamento entre os cidadãos europeus.

Metodologia: O texto foi elaborado enquanto se aguardava a resposta do TJUE relativamente às questões prejudiciais formuladas por dois tribunais nacionais (um sueco e outro britânico) quanto aos efeitos da declaração de invalidade da Diretiva 2006/24 na legislação interna que a transpôs. Assim, os autores procuraram antecipar a decisão do TJUE a partir da análise da sua jurisprudência assente, bem como da reação das autoridades dos Estados-Membros na sequência da declaração de invalidade da referida diretiva.

Resultados: Os autores julgam ter traçado, à luz das particularidades da proteção dos direitos fundamentais na UE e do modelo jurídico da integração, linhas orientadoras quanto ao procedimento a adotar em casos futuros, por forma a salvaguardar a efetividade do direito da União assim como a igualdade jurídica dos cidadãos europeus.

Palavras-chave: conservação de dados, comunicações eletrónicas, direitos fundamentais, direito da União Europeia.

Abstract

Purpose *– The text deals with the recent case law of the European Court of Justice (ECJ) on the directive on the retention of data (metadata) by providers of electronic communications services for the purposes of investigation, detection and prosecution of serious crimes. The authors seek to clarify the implications of the declaration of*

[*]Diretora do Centro de Estudos em Direito da União Europeia (CEDU) da Universidade do Minho. Titular da Cátedra Jean Monnet em Direito da União Europeia. Email: asilveira@direito.uminho.pt.
[**]Professor na Escola de Direito da Universidade do Minho. Email: pfreitas@direito.uminho.pt.

invalidity of this European directive for the EU Member States, towards the protection of legal equality of European citizens.
Methodology/approach/design – *The text was drafted while there was a pending ECJ's response to the questions referred by two national courts (one Swedish and one British) on the effects of that invalidity decision on the domestic legislation that transposed it. Thus, the authors sought to anticipate the Court's decision in the light of its settled case law and the reaction of the Member States' authorities' after the declaration of invalidity of the referred directive.*
Findings – *In the light of the particularities of the protection of fundamental rights in the EU and the legal model of integration, the authors draw some guidelines as to the procedure to be followed in future cases in order to safeguard the effectiveness of the Union law, namely when it comes to the legal equality of European citizens.*

Keywords: conservation of data, electronic communications, fundamental rights, European Union law.

Introdução

No acórdão *Digital Rights Ireland* de 2014[1], o Tribunal de Justiça da União Europeia (TJUE) declarou a invalidade da Diretiva 2006/24 (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). Esta diretiva não regulava o tratamento de dados pelas autoridades públicas ou policiais dos Estados-Membros, mas sim a conservação de dados por fornecedores de serviços no exercício de atividades económicas para efeitos de investigação, de deteção e de repressão de infrações graves, independentemente de qualquer pedido prévio de acesso por parte das autoridades policiais ou judiciárias dos Estados-Membros.[2] Os dados em causa permitem saber com quem um utilizador comunicou, através de que meio, o tempo da comunicação, o local a partir do qual a comunicação se efetuou, e com que frequência um utilizador comunica com certas pessoas durante um determinado período – informações conhecidas por "metadados" (GUILD; CARRERA, 2014, p. 1). A diretiva era aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares quer a pessoas coletivas

[1]Acórdão *Digital Rights Ireland*, de 8 de abril de 2014, processos apensos C-293/12 e C-594/12 (disponível em www.curia.europa.eu).
[2]As disposições da Diretiva 2006/24 visavam à aproximação das legislações nacionais relativas à obrigação de conservação de dados (artigo 3.°), às categorias de dados a conservar (artigo 5.°), ao período de conservação dos dados (artigo 6.°), à proteção e à segurança dos dados (artigo 7.°), bem como aos requisitos para a sua armazenagem (artigo 8.°).

(no Brasil, pessoas jurídicas), incluindo as informações consultadas utilizando uma rede de comunicações eletrónicas, não sendo, todavia, aplicável ao conteúdo das comunicações. De qualquer forma, os Estados-Membros deviam assegurar que os dados fossem conservados por períodos não inferiores a seis meses e não superiores a dois anos, a contar da data da comunicação, de modo que tais dados pudessem ser transmitidos imediatamente, mediante pedido, às autoridades competentes.

O cerne da questão residia no fato de que a diretiva abrangia *todos* aqueles que utilizassem serviços de comunicações eletrónicas na Europa – sem que as pessoas cujos dados eram conservados se encontrassem numa situação suscetível de dar lugar a ações penais. Além disso, a diretiva não previa qualquer diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações graves, pelo que era aplicável mesmo a pessoas cujas comunicações estivessem sujeitas ao segredo profissional. A esta ausência geral de limites acresce que a Diretiva 2006/24 não estabelecia um critério objetivo que permitisse delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior. Ademais, a diretiva não impunha que os dados em causa fossem conservados no território da União, pelo que não se podia considerar que estivesse plenamente garantida a fiscalização por uma entidade independente. Em última análise, a diretiva obrigava os fornecedores dos serviços de comunicações eletrónicas a conservarem dados cuja exploração torna possível "a cobertura cartográfica fiel e exaustiva dos comportamentos de uma pessoa abrangidos estritamente pela sua vida privada, ou até um retrato completo e preciso da sua identidade privada".[3]

Ora, uma obrigação geral de conservação de dados nestes termos permite ingerências individuais graves por via de uma vigilância direcionada mas também ingerências em massa porventura ainda mais preocupantes. Isto é, aquelas que afetam uma parte substancial ou mesmo toda a população relevante de um Estado-Membro, como a identificação de todos os indivíduos que sofrem de distúrbios psicológicos ou de todos os indivíduos que se opõem à política do governo. Basta que se identifique instantaneamente todos os indivíduos que contataram um psicólogo durante o período de conservação dos dados ou todos os indivíduos inscritos em listas de distribuição de mensagens de correio eletrónico que criticam a política do governo.[4]

O TJUE foi então chamado a apreciar a validade da Diretiva 2006/24 à luz dos artigos 7.° (proteção da vida privada) e 8.° (proteção de dados pessoais)

[3]Cfr. conclusões (Advogado-Geral Cruz Villalón) *Digital Rights Ireland*, de 12 de dezembro de 2013, proc. C-293/12, considerandos 72 a 74.
[4]Cfr. conclusões *Tele2* (Advogado-Geral Henrik Saugmandsgaard Øe), de 19 de julho de 2016, processos apensos C-203/15 e C-698/15, considerandos 252 a 258.

da Carta dos Direitos Fundamentais da União Europeia (CDFUE) e entendeu que a obrigação imposta pela Diretiva 2006/24 aos fornecedores de serviços de comunicações eletrónicas constituía uma ingerência nos referidos direitos fundamentais[5] – e para tanto, pouco importava que se tratasse (ou não) de dados sensíveis ou que os interessados tivessem (ou não) sofrido inconvenientes em razão dessa ingerência.[6]

O TJUE entendeu que, se é certo que a luta contra a criminalidade grave assume primordial importância para garantir a segurança pública – e que a sua eficácia pode depender da utilização das técnicas modernas de investigação –, tal objetivo de interesse geral, por muito fundamental que seja, não pode por si só justificar que uma medida de conservação como a que foi instituída pela Diretiva 2006/24 seja considerada necessária para os efeitos daquele combate.[7] Nesta medida, o TJUE concluiu que a Diretiva 2006/24 não previa garantias suficientes, como exige o artigo 8.° da CDFUE, que permitissem assegurar uma proteção eficaz dos dados conservados contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos. Com efeito, a Diretiva 2006/24 não estabelecia regras que regulassem o alcance da ingerência nos direitos fundamentais dos titulares dos dados de modo a limitá-la ao estritamente necessário. Ao adotar a Diretiva 2006/24 o legislador da União teria excedido os limites impostos pelo princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1 da CDFUE – razão pela qual o TJUE declarou a invalidade da diretiva na sua totalidade, sem reservas quanto aos efeitos temporais da sua decisão (eficácia *ex tunc*).

A decisão do TJUE suscitou o problema dos efeitos daquela invalidade relativamente às disposições nacionais que transpuseram a diretiva entretanto declarada integralmente inválida. Alguns doutrinadores sugeriram que o impacto da decisão do TJUE sobre as medidas nacionais não era claro – pois o Tribunal não havia dado indicações neste específico caso –, contudo impunha-se o princípio do primado e a consequente conformidade das normas nacionais com o direito da União (BOEHM; COLE, 2014, p. 28). Outros doutrinadores afinaram pelo diapasão tradicional segundo o qual a declaração de invalidade da diretiva não implicaria diretamente a invalidade da lei nacional que a transpôs – na medida em que as normas em causa seriam oriundas de distintas fontes ou ordenamentos jurídicos separados –, sendo todavia imperativo avaliar a conformidade das normas nacionais com o direito da União na sequência da decisão do TJUE (GUERRA; CALVÃO, 2015, p. 79). Diante da dificuldade do

[5]Cfr. acórdão *Digital Rights Ireland*, *cit*., considerando 34.
[6]Cfr. acórdão *Digital Rights Ireland*, *cit*., considerando 33.
[7]Cfr. acórdão *Digital Rights Ireland*, *cit*., considerando 61.

problema, não admira que, na sequência do acórdão *Digital Rights Ireland*, dois tribunais nacionais (um sueco e outro britânico) tenham colocado questões prejudiciais ao TJUE a fim de, em última análise, testar a conformidade de regimes nacionais que continuam a impor uma obrigação geral de conservação de dados a prestadores de serviços de comunicações eletrónicas acessíveis ao público – cujo acórdão foi recentemente publicado.[8] Ou seja, através das referidas questões prejudiciais, o TJUE foi instado a precisar as consequências da invalidade declarada no acórdão *Digital Rights Ireland* para as autoridades nacionais, assim como deslindar se uma obrigação geral de conservação de dados seria compatível com o artigo 15.°, n.° 1, da Diretiva 2002/58 (relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas), à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da CDFUE. O referido artigo 15.°, n.° 1, da Diretiva 2002/58 autoriza os Estados-Membros a adotar medidas legislativas de conservação de dados durante um período limitado, desde que respeitados os princípios gerais do direito da União e os direitos fundamentais por ela protegidos.

Diante do exposto, no presente texto pretendemos equacionar os efeitos da decisão de invalidade da Diretiva 2006/24 para as autoridades nacionais a partir da evolução da teoria dos direitos fundamentais na União Europeia[9] – e da igualdade de posições jurídicas dos cidadãos europeus em que ela assenta – e, nesta medida, demonstrar por que razão defendemos *i*) que a declaração de invalidade das disposições normativas constantes de uma diretiva europeia afeta inelutavelmente o ato legal de transposição da mesma para o ordenamento jurídico interno e *ii*) que um Estado-Membro não pode utilizar a faculdade conferida pelo artigo 15.°, n.° 1 da Diretiva 2002/58 para impor a manutenção de uma obrigação geral de conservação de dados na sequência da declaração de invalidade da Diretiva 2006/24.

Dos efeitos da declaração de invalidade de uma diretiva na ordem jurídica nacional

A declaração de invalidade de uma disposição europeia pelo TJUE em sede de reenvio prejudicial [artigo 267.º do Tratado sobre o Funcionamento da União

[8]Acórdão *Tele2*, de 21 de dezembro de 2016, processos apensos C-203/15 e C-698/15.
[9]Sobre o papel dos direitos fundamentais na ordem jurídica da União Europeia para os efeitos da decisão *Digital Rights Ireland* cfr. Elspeth Guild and Sergio Carrera, The political and judicial life of metadata: Digital Rights Ireland and the trail of the data retention directive, CEPS Papers in Liberty and Security in Europe, 2014 (http://www.ceps.eu); Niklas Vainio and Samuli Miettinen, Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States, in International Journal of Law and Information Technology, 23, 2015.

Europeia (TFUE)] obriga não apenas o juiz nacional que suscitou a questão prejudicial (que não pode aplicar uma disposição europeia considerada inválida pelo TJUE sob pena de criar graves incertezas sobre o direito da União aplicável),[10] mas também todo e qualquer tribunal nacional dos Estados-Membros da União Europeia (pois a declaração de invalidade de uma disposição europeia pelo TJUE constitui razão suficiente para que qualquer outro órgão jurisdicional considere a disposição inválida para os efeitos da decisão que deva proferir).[11] Assim, resulta da jurisprudência assente do TJUE que as autoridades nacionais *i*) não devem aplicar, sob pena de incumprimento do direito da União, uma disposição normativa europeia considerada inválida pelo TJUE e *ii*) devem deduzir em seu ordenamento interno as consequências de uma declaração de invalidade de uma disposição europeia pelo TJUE,[12] podendo, justificadamente, submeter novas questões prejudiciais de validade caso subsistam dúvidas relativas aos motivos, ao alcance ou às consequências da invalidade declarada.[13] Da jurisprudência do TJUE também deriva que a declaração de invalidade produz efeitos retroativos – ou seja, remonta à data da entrada em vigor da norma e surte efeitos desde então (*ex tunc*), salvo se o TJUE entender que ponderosas razões de segurança jurídica justificam a limitação temporal dos efeitos do acórdão (artigo 264.º do TFUE, relativo ao recurso de anulação, aplicado por analogia em sede de reenvio de validade)[14].

Diante do exposto, não é propriamente árduo perceber que a declaração de invalidade das disposições constantes de uma diretiva afeta inelutavelmente o ato legal de transposição da mesma para o ordenamento jurídico interno. Assim o é por força do princípio da lealdade europeia [artigo 4.º, n.º 3 do Tratado da União Europeia (TUE)],[15] do princípio da igualdade e não discriminação em razão da nacionalidade (artigo 18.º do TFUE)[16], assim como da força juridicamente vinculativa das decisões do TJUE – que é a instituição competente para garantir o respeito do direito na interpretação e aplicação dos Tratados

[10]Cfr. acórdão *International Chemical Corporation*, de 13 de maio de 1981, proc. 66/80, considerando 12.
[11]Cfr. acórdão *International Chemical Corporation*, *cit*., considerando 13.
[12]Cfr. acórdão *Rey Soda*, de 30 de outubro de 1975, proc. 23/75, considerando 51.
[13]Cfr. acórdão *International Chemical Corporation*, *cit*., considerando 14.
[14]Cfr. acórdão *Roquette Frères*, de 15 de outubro de 1980, proc. 145/79, considerandos 50-53.
[15]Segundo o qual os Estados-Membros tomam todas as medidas gerais ou específicas adequadas para garantir a execução das obrigações decorrentes dos Tratados ou resultantes dos atos das instituições da União.
[16]Segundo o qual, no âmbito de aplicação dos Tratados, é proibida toda e qualquer discriminação em razão da nacionalidade, o que proíbe as diferenciações de tratamento entre cidadãos europeus sem justificação razoável.

(artigo 19.º, n.º 1 do TUE). Isto significa que um juiz nacional, confrontado com a aplicação de um diploma legislativo interno que transpõe uma diretiva declarada inválida pelo TJUE, terá de o considerar desconforme com o direito da União e declará-lo inaplicável por força do princípio do primado daquele direito (que deriva do princípio da lealdade europeia). Para tal conclusão ainda relevam *i*) os princípios que presidem a repartição de competências entre União e Estados-Membros, máxime o princípio da preclusão (artigo 2.º, n.º 2 do TFUE),[17] mas também e sobretudo *ii*) a ausência de autonomização do direito interno no momento da transposição, pois o diploma legal que transpõe uma diretiva será sempre direito da União Europeia transposto, e não direito de fonte originariamente nacional. Assim, os critérios de interpretação e aplicação das disposições internas que transpõem uma diretiva europeia são definidos pelo direito da União – e vão continuar a sê-lo na sequência da declaração de invalidade de um ato jurídico emitido no exercício das suas competências –,[18] sob pena de comprometer-se a uniformidade/homogeneidade da aplicação do direito da União nos distintos Estados-Membros e, em última análise, a própria igualdade jurídica dos cidadãos europeus.

Ademais, quando a declaração da invalidade de um ato jurídico da União se baseia numa violação de direitos fundamentais, a ponderação dos diferentes interesses em presença deve ser objeto de uma avaliação muitíssimo atenta – impondo-se, sobretudo, a urgência da cessação da restrição aos direitos fundamentais em causa. Aqui relevam as obrigações que impendem sobre o juiz nacional relativas à apreciação da compatibilidade das medidas nacionais de transposição de uma diretiva com as garantias previstas na CDFUE[19]. De resto, o TJUE já esclareceu que quando um órgão jurisdicional de um Estado-Membro é chamado a fiscalizar a conformidade jusfundamental de uma medida nacional que aplica o direito da União na aceção do artigo 51.°, n.° 1 da CDFUE,[20] *mas a ação dos Estados-Membros não é inteiramente determinada pelo direito da União*, as autoridades e os órgãos jurisdicionais nacionais podem aplicar os

[17]Segundo o qual, no domínio das competências partilhadas entre União e Estados-Membros, estes exercem a sua competência na medida em que a União não tenha exercido a sua, e apenas voltam a exercê-la na medida em que a União tenha decidido deixar de exercer a sua.

[18]Neste sentido, cfr. conclusões *Tele 2*, *cit.*, considerando 191, no qual o Advogado-Geral explica que é impossível interpretar as disposições da CDFUE de modo distinto consoante o regime em causa tenha sido estabelecido a nível da União ou a nível nacional, razão pela qual os critérios desenvolvidos pelo TJUE no acórdão *Digital Rights Ireland* são relevantes para efeitos da apreciação dos regimes nacionais sobre conservação de dados.

[19]Cfr. conclusões *Digital Rights Ireland*, *cit.*, considerando 153.

[20]Segundo o qual as disposições da Carta têm como destinatários os Estados-Membros quando apliquem o direito da União.

padrões nacionais de proteção dos direitos fundamentais, *desde que essa aplicação não comprometa o nível de proteção previsto pela Carta conforme interpretado pelo TJUE, nem o primado, a unidade e a efetividade do direito da União.*[21] Ora, diante da declaração de invalidade de uma diretiva com fundamento na violação de direitos fundamentais protegidos pela União, as normas nacionais que a transpõem não conseguem passar pelo teste de conformidade com o padrão de jusfundamentalidade resultante da CDFUE nos termos referidos *supra*.[22]

Não foi por outra razão que o TJUE não acolheu a sugestão do Advogado-Geral Cruz Villalón relativa à suspensão dos efeitos da declaração de invalidade da Diretiva 2006/24 até que o legislador da União tomasse as medidas necessárias para sanar a invalidade declarada.[23] No entendimento do Advogado-Geral, a Diretiva 2006/24 devia ser considerada inválida devido à inexistência de um enquadramento suficiente das garantias que regulam o acesso aos dados recolhidos e conservados e a sua exploração – mas tal vício poderia, porventura, ser corrigido no âmbito das medidas de transposição adotadas pelos Estados-Membros até que o legislador da União atuasse em conformidade com o acórdão.[24] Todavia, o TJUE rejeitou tal sugestão e declarou a diretiva inválida na sua totalidade, sem reservas quanto aos efeitos da sua decisão no tempo, seja para ressalvar efeitos já produzidos seja para manter a vigência do ato inválido até a sua substituição. De resto, o TJUE tem procurado esclarecer que o objetivo da proteção dos direitos fundamentais no direito da União é zelar por que tais direitos não sejam violados nos domínios de atividade da União, seja em razão da ação da União ou em razão da aplicação do direito da União pelos Estados-Membros.[25] No entendimento do TJUE, a prossecução deste objetivo justifica-se pela necessidade de evitar que o distinto nível de proteção dos direitos fundamentais, suscetível de variar consoante o direito nacional em causa, prejudique a unidade, o primado e efetividade do direito da União.[26] O TJUE estabelece, portanto, uma nítida conexão entre a proteção dos direitos fundamentais – tal como a CDFUE os contempla – e o imperativo de efetividade

[21]Cfr. acórdão *Melloni*, de 26 de fevereiro de 2013, proc. C-399/11, considerando 60 e acórdão *Fransson*, de 26 de fevereiro de 2013, proc. C-617/10, considerando 29.
[22]Neste sentido cfr. Franziska Boehm and Mark D. Cole, *Data Retention after the Judgement of the Court of Justice of the European Union*, *cit.*: "It is therefore hardly imaginable that a Member State transposing act that follows the structure and content of the core provisions of the DRD can remain unchanged without itself being in violation of the fundamental rights standards set by the Court in its judgement."
[23]Cfr. conclusões *Digital Rights Ireland*, *cit.*, considerando 158.
[24]Cfr. conclusões *Digital Rights Ireland*, *cit.*, considerando 157.
[25]Cfr. acórdão *Siragusa*, de 6 de março de 2014, proc. C-206/13, considerando 31.
[26]*Idem.*

do direito da União. Está aqui patente a ideia de que as dissonâncias na proteção dos direitos fundamentais nos distintos Estados-Membros poderiam comprometer a igualdade jurídica dos cidadãos europeus – e, em última análise, a própria sobrevivência de uma União de direito. Por conseguinte, na sequência do acórdão *Digital Rights Ireland*, cumpre às autoridades nacionais não aplicar as normas internas de transposição da diretiva considerada inválida.

Ora, no exercício de competências partilhadas relativas ao mercado interno [artigo 4.º, n.º 2, alínea *a)* e artigo 114.º do TFUE] tanto a União como os Estados-Membros podem legislar e adotar atos juridicamente vinculativos. Mas decorre do artigo 2.º, n.º 2 do TFUE que a atuação da União preclude/inibe a atuação dos Estados-Membros. Ou seja, os Estados exercem a sua competência na medida em que a União não tenha exercido a sua – e apenas voltam a exercê-la na medida em que a União tenha decidido deixar de exercer a sua. Nada disso aconteceu para que os Estados-Membros passem a exercer as suas competências partilhadas no domínio da proteção de dados ignorando as disposições europeias, sobretudo porque a competência da União em matéria de proteção de dados pessoais (artigo 16.º do TFUE) vem sendo exercida/concretizada desde a Diretiva 95/46 (relativa o tratamento de dados e a sua circulação no espaço da União). Na realidade, a Diretiva 2006/24 (declarada inválida) impunha uma obrigação de recolha e de conservação dos dados de tráfego e de localização que se inscrevia no âmbito dos limites ao direito à proteção dos dados pessoais previstos no artigo 13.°, n.º 1 da Diretiva 95/46 (relativa o tratamento de dados e a sua circulação no espaço da União) e artigo 15.°, n.º 1 da Diretiva 2002/58 (relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas), visto que estas diretivas consagram a confidencialidade das comunicações e dos dados relativos ao tráfego, bem como a obrigação de os eliminar ou tornar anónimos.[27] De resto, no acórdão *Irlanda contra Parlamento e Conselho* de 2009[28] o TJUE explica que, antes da adoção da Diretiva 2006/24, diversos Estados-Membros tinham tomado, nos termos do artigo 15.°, n.° 1 da Diretiva 2002/58, medidas nacionais relativas à conservação de dados com diferenças significativas entre si, com períodos de conservação que variavam entre três meses, nos Países Baixos, e quatro anos, na Irlanda. Ora, as obrigações relativas à conservação de dados têm implicações económicas importantes para os fornecedores de serviços – e as divergências entre essas obrigações podem causar distorções no mercado interno europeu. Neste contexto, impôs-se a adoção da Diretiva 2006/24 com base no (atual) artigo 114.º do TFUE.

[27]Cfr. conclusões *Digital Rights Ireland, cit.*, considerandos 35-36.
[28]Cfr. acórdão *Irlanda contra Parlamento Europeu e Conselho da União Europeia*, de 10 de fevereiro de 2009, proc. C- 301/06, considerando 50.

Assim, diante da invalidade da Diretiva 2006/24, foram afastadas as derrogações nela previstas ao artigo 5.º (confidencialidade das comunicações), ao artigo 6.º (dados de tráfego) e ao artigo 9.º (dados de localização) da Diretiva 2002/58 (GUERRA; CALVÃO, 2015, p. 79) – e o regime jurídico de conservação de dados (porventura) aplicável nos distintos Estados-Membros teria de ser necessariamente balizado pelos *standards* de proteção definidos no artigo 15.º, n.º 1, da Diretiva 2002/58[29], designadamente os princípios gerais do direito da União e os direitos fundamentais por ela protegidos, tal como interpretados pelo TJUE. Dentro de tais condicionantes, o artigo 15.º, n.º 1, da Diretiva 2002/58 prevê que os Estados-Membros podem adotar medidas legislativas que prevejam a conservação de dados durante um período limitado para efeitos de prevenção, investigação, deteção e repressão de infrações penais. Mas certamente *não* nos termos de uma obrigação geral de conservação de dados como aquela que resultava da Diretiva 2006/24 – que, de resto, aditou o artigo 15.°, n.° 1-A à Diretiva 2002/58, segundo o qual o artigo 15.°, n.° 1, da Diretiva 2002/58 seria inaplicável ao regime de conservação geral previsto na Diretiva 2006/24. Ou seja, para os efeitos de uma obrigação geral de conservação de dados, foi necessária a emissão de uma diretiva própria porque o artigo 15.º, n.º 1, da Diretiva 2002/58 não servia. A Diretiva 2006/24 surgiu precisamente para limitar, de forma harmonizada a nível europeu, as obrigações previstas na Diretiva 2002/58[30]. Daqui deriva que o artigo 15.°, n.° 1, da Diretiva 2002/58 não pode ser interpretado no sentido de permitir a subsistência de uma obrigação geral de conservação de dados que a declaração de invalidade da Diretiva 2006/24 afastou.

[29]Segundo o qual "Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos números 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas restrições constituam uma medida necessária, 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 deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva 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 números 1 e 2 do artigo 6.º do Tratado da União Europeia."

[30]Cfr. acórdão *Irlanda contra Parlamento Europeu e Conselho da União Europeia*, *cit*., considerando 51.

Da reação dos Estados-Membros na sequência da declaração de invalidade da Diretiva 2006/24

Contudo, na sequência do acórdão *Digital Rights Ireland* a reação dos Estados-Membros não foi consensual – o que acarretou uma diferenciação ilegítima de tratamento entre os cidadãos europeus. Conforme a Nota Prática n.º 7 emitida pelo Ministério Público português (GABINETE CIBERCRIME DO MINISTÉRIO PÚBLICO, 2015), dez dos Estados-Membros da União Europeia declararam inválidas as leis nacionais que transpunham a diretiva da retenção de dados, seja por decisão parlamentar ou dos seus tribunais constitucionais. Nos restantes Estados-Membros, de entre os quais Portugal, não aconteceu assim por entender-se que as exigências substanciais da decisão do TJUE estavam previamente satisfeitas (VAINIO; MIETTINEN, 2015, p. 301 e ss.). Segundo a referida Nota Prática, o entendimento comum, pacificamente partilhado pela comunidade judiciária e pelos operadores de telecomunicações portugueses, é o de que a Lei n.º 32/2008 está em vigor – e, aparentemente, não suscita dúvidas. Alegadamente porque, além da transposição da Diretiva 2006/24, aquela lei introduziu um mais alargado quadro 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 aos dados, ou ainda as condições de armazenamento e de acesso aos dados). Por isso, no entendimento do Ministério Público português, a lei nacional teria ido muito além das exigências da diretiva e "a maior parte das exigências que vieram a ser feitas pelo acórdão do TJUE estariam já anteriormente consideradas no direito interno."[31]

Ocorre que a competência para corrigir os vícios e regular a matéria em conformidade com o acórdão do TJUE não é do legislador português – é do legislador europeu. E assim o é precisamente para evitar o resultado esquizofrénico segundo o qual, no âmbito de uma competência europeia, os cidadãos de outro Estado-Membro que não Portugal, insuspeitos da prática de um crime, já não sejam alvo de retenção dos seus dados pessoais no seguimento do acórdão *Digital Rights Ireland*, e os portugueses ainda o sejam. Ora, isto mina a efetividade do direito da União, compromete a homogeneidade da sua aplicação nos distintos Estados-Membros, e provoca diferenciações de tratamento injustificadas entre os cidadãos europeus em matéria de proteção dos seus direitos fundamentais. A disparidade de soluções registadas entre os distintos Estados-Membros na sequência da declaração de invalidade da Diretiva 2006/24 sugere a existência de graves divergências quanto ao direito da União

[31]Para a análise das contradições da Lei n.º 32/2008 com o direito da União Europeia cfr. Clara Guerra e Filipa Calvão, Anotação acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014, *cit*., p. 81-82.

aplicável – o que resulta incompatível com a ideia de uma União de direito. Neste contexto, caso subsistissem fundadas dúvidas aos tribunais portugueses quanto à continuidade da aplicação da Lei n.º 32/2008, impunha-se o diálogo com o TJUE via reenvio prejudicial a fim de *i*) desvendar o alcance ou consequências da invalidade declarada e *ii*) afastar o risco de interpretação equivocada/violação do direito da União – de resto, passível de responsabilização por exercício da função jurisdicional.[32] Ou, no mínimo, impunha-se a suspensão da instância porquanto tramitavam no TJUE dois reenvios prejudiciais sobre a matéria[33] – relativamente aos quais as autoridades portuguesas não podiam alegar desconhecimento porque, nos termos do artigo 21.º, n.º 4 do Regulamento de Processo do Tribunal de Justiça, é publicada uma comunicação no *Jornal Oficial da União Europeia* dando conta das questões prejudiciais submetidas ao Tribunal, sendo o Estado português notificado para a apresentação de alegações ou observações escritas nos termos do artigo 96.º, n.º 1, *b)* do referido Regulamento.

Todavia, discordando da decisão do TJUE, a Nota Prática n.º 7 do Ministério Público português afirma que a decisão daquele Tribunal impõe "condições que não são viáveis ou que, sendo-o, tornam a retenção inútil." Neste sentido, é defendido que a retenção de dados, tal como é entendida no quadro da Diretiva 2006/24 e da Lei nº 32/2008, apenas é útil se os dados se referirem a todos os cidadãos, de forma indiscriminada, pois "no momento em que os dados são retidos e conservados, não é possível saber se, porventura, aqueles dados poderão vir a ser necessários, como prova de um crime. Somente após ter ocorrido um crime, os dados entretanto retidos de forma generalizada e indiscriminada assumirão valor probatório". Todavia, decorre do acórdão *Digital Rights Ireland* que o Governo português, nas observações escritas que apresentou ao TJUE, teria relativizado a eficácia do regime de recolha dos dados de tráfego e de localização imposto pela Diretiva 2006/24, sobretudo no que se refere à criminalidade organizada e ao terrorismo, em função de existirem várias modalidades de comunicações eletrónicas que não estão abrangidas pelo seu âmbito de aplicação ou que permitem uma comunicação anónima, sendo perfeitamente possível escapar à sua influência – o que limita a adequação da medida de conservação dos dados à realização do objetivo prosseguido.[34] Ora, se assim é, por que motivo submeter os cidadãos portugueses insuspeitos da prática de um crime a uma vigilância permanente e indiscriminada? Com que

[32]Cfr. acórdão *Ferreira da Silva*, de 9 de setembro de 2015, proc. C-160/14, considerando 44.
[33]Processos apensos C-203/15 e C-698/15.
[34]Cfr. conclusões *Digital Rights Ireland, cit.*, considerando 50.

justificativa gerar nos portugueses a sensação de que a sua vida privada é constantemente vigiada, visto que a conservação dos dados e a sua utilização posterior são efetuadas sem que o utilizador seja disso informado quer pelos fornecedores de serviço quer pelas autoridades públicas que acedem aos dados?[35]

A Diretiva 2006/24 impunha uma obrigação aos fornecedores de serviços de comunicações eletrónicas – qual seja, a de recolher e de conservar os dados de tráfego e de localização daquelas comunicações –, mas não previa as garantias que deviam regular o acesso aos referidos dados conservados e a sua exploração, remetendo o tratamento desta matéria, genericamente, para os Estados-Membros. Eis, portanto, o busílis identificado pelo TJUE[36]. Ora, quando a restrição de direitos fundamentais tem origem na legislação da própria União e, por conseguinte, esta lhe é imputável, é o legislador da União quem deve desempenhar um papel diretor na definição das referidas garantias – sob pena de esvaziar de sentido as disposições do artigo 51.º, n.º 1, da CDFUE –, competindo aos Estados-Membros, caso a matéria seja regulada através de uma diretiva, a pormenorização das garantias que devem regular a restrição dos direitos fundamentais.[37] Mas sempre a partir do padrão de jusfundamentalidade definido pela União, pois resulta da jurisprudência constante do TJUE que os direitos fundamentais garantidos pela ordem jurídica europeia são aplicáveis em todas as situações reguladas pelo direito da União – e a obrigação de respeitar os direitos fundamentais definidos no quadro europeu se impõe aos Estados-Membros quando estes atuam no âmbito de aplicação do direito da União. Assim, a aplicabilidade do direito da União implica necessariamente a aplicabilidade dos direitos fundamentais garantidos pela CDFUE.[38]

Por conseguinte, a União não pode instituir uma medida como a obrigação duradoura de recolha e de conservação de dados sem, simultaneamente, a enquadrar através de garantias quanto às condições a que o seu acesso e exploração ficam sujeitos. É justamente este enquadramento das condições de acesso e de exploração dos dados recolhidos e conservados que permite apreciar o alcance que esta ingerência implica – e que pode torná-la (jus)fundamentadamente aceitável ou não.[39] Assim, no entender do TJUE, competia ao legislador europeu:

[35]Cfr. acórdão *Digital Rights Ireland, cit.*, considerando 37.
[36]Cfr. conclusões *Digital Rights Ireland, cit.*, considerando 113.
[37]Cfr. concusões *Digital Rights Ireland, cit.*, considerandos 117 e 120.
[38]Cfr. acórdão *Fransson*, de 26 de fevereiro de 2013, proc. C-617/10, considerandos 19-21.
[39]Cfr. conclusões *Digital Rights Ireland, cit.*, considerando 121.

i) estabelecer regras claras e precisas que regulassem o âmbito e a aplicação da medida em causa[40] (descrevendo as atividades criminais suscetíveis de justificarem o acesso aos dados conservados com um maior grau de precisão do que através da expressão "infrações graves"),[41] assim como o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da CDFUE;[42]

ii) estabelecer limites quanto aos dados conservados relativamente a um período de tempo, a uma zona geográfica, e/ou a um círculo de pessoas determinadas que possam estar implicadas numa infração grave;[43]

iii) estabelecer critérios objetivos (condições materiais e processuais) que permitissem delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas suficientemente graves;[44]

iv) estabelecer critérios objetivos que permitissem limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados e que sujeitassem dito acesso a um controle prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente na sequência de um pedido fundamentado; [45]

v) estabelecer que a determinação do período de conservação deve basear-se em critérios objetivos tendo em conta a distinção entre as categorias de dados a conservar;[46]

vi) garantir a aplicação de um nível particularmente elevado de proteção e segurança pelos fornecedores e a destruição definitiva dos dados no termo do período de conservação dos mesmos;[47]

vii) impor que os dados em causa fossem conservados no território da União.[48]

O Advogado-Geral no processo *Digital Rights Ireland* ainda lembrou que o legislador da União devia ter instituído a obrigação de que as autoridades

[40]Cfr. acórdão *Digital Rights Ireland, cit.*, considerando 54.
[41]Cfr. conclusões *Digital Rights Ireland, cit.*, considerando 126 e acórdão *Digital Rights Ireland, cit.*, considerando 60.
[42]Cfr. acórdão *Digital Rights Ireland, cit.*, considerando 65.
[43]Cfr. acórdão *Digital Rights Ireland, cit.*, considerando 59.
[44]Cfr. acórdão *Digital Rights Ireland, cit.*, considerandos 60 e 61.
[45]Cfr. acórdão *Digital Rights Ireland, cit.*, considerando 62.
[46]Cfr. acórdão *Digital Rights Ireland, cit.*, considerandos 63 e 64.
[47]Cfr. acórdão *Digital Rights Ireland, cit.*, considerando 67.
[48]Cfr. acórdão *Digital Rights Ireland, cit.*, considerando 68.

autorizadas a aceder aos dados informassem tal acesso aos titulares dos mesmos depois de afastado o risco de que tal informação afetasse a eficácia das medidas que justificaram a exploração dos dados.[49] Neste sentido, o artigo 13.º da (nova) Diretiva 2016/680 (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados) regula a matéria das informações a facultar ou a fornecer ao titular dos dados. Os Estados-Membros têm até 6 de maio de 2018 para adotar as disposições legislativas, regulamentares e administrativas necessárias ao cumprimento da diretiva. Todavia, sendo destinatários das disposições da diretiva desde a sua entrada em vigor (qual seja, o dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* em 4 de maio de 2016), as autoridades nacionais, máxime os seus órgãos jurisdicionais, são obrigados a prosseguir as finalidades da diretiva, empenhando-se na interpretação do direito nacional em conformidade com o espírito da mesma (princípio da interpretação conforme ao direito da União).

Da restrição ao exercício de direitos fundamentais previstos na CDFUE

De qualquer forma, e apesar de ser um marco na jurisprudência do TJUE sobre proteção de direitos fundamentais – comparável, segundo Steve Peers (2014), aos clássicos acórdãos sobre direitos civis da Suprema Corte dos EUA[50] –, o acórdão *Digital Rights Ireland* não pôs termo à retenção de dados no contexto da União (VAINIO; MIETTINEN, 2015, p. 308), sobretudo porque o TJUE entendeu que, embora a conservação dos dados imposta pela Diretiva 2006/24 constituísse uma ingerência particularmente grave nos direitos fundamentais à proteção da vida privada e à proteção de dados pessoais, não era suscetível de afetar o conteúdo essencial de tais direitos. Ora, em conformidade com o artigo 52.°, n.° 1, da CDFUE, qualquer restrição ao exercício dos direitos e liberdades nela previstos deve *i*) ser prevista por lei, *ii*) respeitar o conteúdo essencial daqueles direitos, *iii*) respeitar o princípio da proporcionalidade, e *iv*) ser necessária à prossecução dos objetivos de interesse geral reconhecidos pela União ou à proteção de direitos e liberdades de terceiros. Todavia, tendo em conta que o artigo 1.°, n.° 2, da Diretiva 2006/24 não permitia que se tomasse

[49]Cfr. conclusões *Digital Rights Ireland*, *cit.*, considerando 129.

[50]De acordo com Steve Peers, The data retention judgment: the CJEU prohibits mass surveillance, in *EU law analysis*, 8 de abril de 2014: "Time will deal whether the *Digital Rights* judgment is seen as the EU's equivalent of classic civil rights judgments of the US Supreme Court, on the desegregation of schools (*Brown*) or criminal suspects' rights (*Miranda*). If the Charter ultimately contributes to the development of a 'constitutional patriotism' in the European Union, this judgment will be one of its foundations".

conhecimento do conteúdo das comunicações eletrónicas, o TJUE entendeu que não havia comprometimento do núcleo essencial do direito à privacidade. Acresce, no entendimento do TJUE, que o artigo 7.° da Diretiva 2006/24 previa o respeito a princípios de proteção e de segurança dos dados pessoais, de acordo com os quais os Estados-Membros deviam assegurar a adoção de medidas técnicas e organizacionais contra a destruição acidental ou ilícita, a perda ou a alteração acidental dos dados – e por isso o núcleo essencial do direito fundamental à proteção de dados também estaria salvaguardado[51]. Todavia, ainda que o núcleo essencial estivesse salvaguardado, a legislação era desproporcionada – eis o entendimento do TJUE que esteve na base da declaração de invalidade da Diretiva 2006/24.

Ocorre que não é adquirido, à luz da jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH), que o caráter geral e indiferenciado da conservação de dados pessoais pelos fornecedores de serviços de comunicações eletrónicas (vigilância generalizada) respeite o núcleo essencial dos direitos em causa – sobretudo porque a suspeição não é um elemento necessário para a justificação da retenção dos dados. E tão pouco o é à luz das tradições constitucionais comuns aos Estados-Membros, tendo em conta as decisões de inconstitucionalidade de normas nacionais proferidas por vários tribunais constitucionais dos Estados-Membros na sequência da declaração de invalidade da Diretiva 2006/24 pelo TJUE. No acórdão do TEDH *S. e Marper contra Reino Unido*,[52] por exemplo, em que estava em causa a conservação de perfis genéticos (ADN) ou de impressões digitais de qualquer pessoa absolvida da prática de um crime ou cujo processo tenha sido arquivado sem condenação, o TEDH entendeu que a retenção em si mesma era contrária à Convenção Europeia dos Direitos do Homem (CEDH), independentemente da consideração das salvaguardas previstas (WHITE, 2016). E no acórdão *Roman Zakharov contra Russia*,[53] em que estava em causa o sistema russo de intercetação de comunicações telefónicas, o TEDH decidiu que a conservação automática por seis meses de dados claramente irrelevantes não se justificava à luz do artigo 8.º da CEDH (respeito pela vida privada).[54] Este sentido decisório pode porventura

[51]Cfr. acórdão *Digital Rights Ireland, cit.*, considerandos 38-40.
[52]Cfr. acórdão *S. e Marper contra Reino Unido*, de 4 de dezembro de 2008, processos 30562 e 30566/04, considerando 125.
[53]Cfr. acórdão *Roman Zakharov contra Russia*, de 4 de dezembro de 2015, proc. 47143/06, considerando 255.
[54]Comentando tal decisão do TEDH, o Advogado-Geral sublinhou, em *Tele 2*, considerando 243, que os Estados-Membros devem prever a obrigação de destruição definitiva de todos os dados conservados a partir do momento em que já não sejam estritamente necessários na luta contra as infrações graves. Acrescenta que esta obrigação

contrastar com o entendimento do TJUE no acórdão *Digital Rights Ireland* sobre a não afetação do núcleo essencial dos direitos fundamentais em causa – e, numa futura apreciação, levar o TEDH a distanciar-se da doutrina da presunção de proteção equivalente que tem sido acolhida desde o acórdão *Bosphorus contra Ireland*,[55] segundo a qual um Estado signatário respeita as exigências da CEDH sempre que se limita a dar execução às obrigações jurídicas que resultam da sua adesão à União Europeia.

Nas suas Conclusões no processo *Tele 2*,, o Advogado-Geral afinou pelo mesmo diapasão do acórdão *Digital Rights Ireland* quanto à questão da não afetação do núcleo essencial.[56] Todavia, o Advogado-Geral entra manifestamente em contradição quando ressalta que "os riscos ligados ao acesso aos dados relativos às comunicações (ou «metadados») podem ser equivalentes, ou inclusivamente superiores, aos que resultam do acesso ao conteúdo destas comunicações, conforme salientaram a Open Rights Group e a Privacy Internacional, a Law Society of England and Wales, bem como um recente relatório do Alto Comissariado das Nações Unidas para os Direitos do Homem." Em particular, acrescenta o Advogado-Geral, "os «metadados» permitem catalogar quase instantaneamente uma população no seu conjunto, o que o conteúdo das comunicações não permite".[57] Mas então, se a justificativa para não afetar o núcleo essencial do direito à proteção da vida privada residia sobretudo na salvaguarda do conteúdo das comunicações, em que ficamos? O Advogado-Geral arremata afirmando que os riscos de acesso abusivo ou ilegal aos dados conservados nada têm de teórico, pois o risco de acesso abusivo pelas autoridades competentes deve ser relacionado com os números extremamente elevados de pedidos de acesso evocados nas observações apresentadas ao TJUE.[58] No âmbito do regime sueco, a *Tele2* indicou que recebia cerca de 10.000 pedidos de acesso por mês, número que não inclui os pedidos recebidos por outros prestadores ativos no território sueco. No que respeita ao regime do Reino Unido, foram reproduzidos excertos de um relatório oficial que refere 517.236 autorizações e 55.346 autorizações orais urgentes, isto só no ano de 2014. Ademais, reconhece o Advogado-Geral, "o risco de acesso ilegal, por qualquer pessoa, é consubstancial à própria existência de bases de dados conservadas em suportes informáticos".[59] Mas então, se a justificativa para não afetar o núcleo essencial do direito à proteção de dados residia sobretudo nas

deve ser respeitada não apenas pelos prestadores que conservam os dados, mas também pelas autoridades que tiveram acesso aos dados conservados.

[55]Cfr. acórdão *Bosphorus contra Irlanda*, de 30 de junho de 2005, proc. 45036/98.

[56]Cfr. conclusões *Tele2, cit.*, considerandos 156-159.

[57]Cfr. conclusões *Tele2, cit.*, considerando 259.

[58]Cfr. conclusões *Tele2, cit.*, considerando 260.

[59]*Idem.*

medidas contra a destruição acidental ou ilícita, a perda ou a alteração acidental dos dados, em que ficamos?

Não é propriamente árduo perceber que o Advogado-Geral evita admitir que a retenção generalizada e indiferenciada de dados pessoais é *per se* incompatível com os direitos fundamentais protegidos na CDFUE. Por isso concentra atenções nas garantias que devem enformar uma obrigação geral de conservação de dados a fim de que seja compatível com os direitos fundamentais previstos no direito da União – e não propriamente naquilo que os Estados-Membros estariam proibidos de fazer neste domínio (WHITE, 2016). Lamentavelmente, esta espécie de "fuga para a frente" começa a ser habitual no tratamento da matéria – e também teria orientado, segundo a opinião divergente do Juiz Paulo Pinto Albuquerque, o sentido decisório do TEDH no acórdão *Szabó e Vissy contra Hungria*, sobre vigilância generalizada por razões de inteligência e segurança nacional.[60] De qualquer forma, de entre as contradições do Advogado-Geral no processo *Tele 2*, porventura a que nos suscita maior perplexidade seria aquela que se prende com a análise da proporcionalidade em sentido estrito (ou justa medida) de uma obrigação geral de conservação de dados. Esta dimensão não foi apreciada pelo TJUE no acórdão *Digital Rights Ireland* porque o Tribunal entendeu que o regime estabelecido pela Diretiva 2006/24 excedia o necessário para os efeitos da luta contra as infrações graves. Segundo o Advogado-Geral, a exigência de proporcionalidade *stricto sensu* decorre simultaneamente do artigo 15.°, n.° 1, da Diretiva 2002/58, do artigo 52.°, n.° 1, da CDFUE e de jurisprudência constante do TJUE – e implica que uma restrição de direitos fundamentais apenas seja considerada proporcionada se os inconvenientes por ela causados não forem desmesurados face aos objetivos prosseguidos. Assim, a exigência de proporcionalidade *stricto sensu* impõe a ponderação entre as vantagens resultantes da medida à luz do objetivo legítimo prosseguido (por um lado) e os inconvenientes que daí

[60]Cfr. acórdão *Szabó e Vissy contra Hungria*, de 12 de janeiro de 2016, proc. 37138/14, sobretudo o considerando 20 da opinião divergente, no qual Paulo Pinto Albuquerque denuncia aquilo que considera «an illusory conviction that global surveillance is the *deus ex machina* capable of combating the scourge of global terrorism. Even worse, such delusory language obliterates the fact that the vitrification of society brings with it the Orwellian nightmare of *1984*. In practice, the Chamber is condoning, to use the words of the European Parliament, "the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law-enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence"».

decorrem para os direitos fundamentais consagrados numa sociedade democrática (por outro). Ou seja, impõe a ponderação entre as vantagens e os inconvenientes de uma obrigação geral de conservação de dados aplicada a todos os utilizadores europeus sem que seja exigida qualquer suspeita de infração grave – o que, em última análise, daria origem a um debate sobre os valores prevalecentes e sobre o tipo de sociedade em que desejamos viver.[61] Todavia, sem tirar as devidas ilações da proporcionalidade em sentido estrito que enuncia, o Advogado-Geral lava as mãos – qual Pôncio Pilatos – e propõe a seguinte solução em detrimento da homogeneidade aplicativa do direito da União: que se devolva tal apreciação valorativa ao juiz nacional, à luz das garantias imperativas enunciadas pelo TJUE nos considerandos 60 a 68 do acórdão *Digital Rights Ireland* [62] – e salve-se quem puder…

Contrariando a sugestão do Advogado-Geral, no acórdão *Tele 2* o TJUE entendeu basear-se da proporcionalidade em sentido estrito para decidir que a CDFUE se opõe a uma normativa nacional que estabeleça, com a finalidade de lutar contra a delinquência, a conservação generalizada e indiferenciada de *todos* os dados de tráfego e de localização de *todos* os utilizadores registados relativamente a *todos* os meios de comunicação eletrónica.[63] Assim, respondendo mais concretamente às questões formuladas pelos tribunais nacionais em sede de reenvio prejudicial, o TJUE decidiu que o artigo 15.º, n.º1, da Diretiva 2002/58, à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º1, da CDFUE, deve ser interpretado no sentido de que se opõe a uma normativa nacional que regula a proteção de dados de tráfego e de localização, em particular o acesso das autoridades nacionais aos dados conservados, *i*) sem limitar tal acesso aos casos de delinquência grave, *ii*) sem submeter tal acesso ao controlo prévio de um órgão jurisdicional ou uma autoridade administrativa independente, bem como *iii*) sem exigir que os dados em causa se conservem no território da União.[64] O TJUE não alterou a sua posição quanto à ausência de violação do núcleo essencial dos direitos fundamentais em causa. Não obstante, procedeu a um exercício de ponderação via proporcionalidade em sentido estrito que o levou a admitir, inclusivamente, que a conservação dos dados de tráfego e localização poderia influir no uso dos meios de comunicação eletrónica e, por conseguinte, no exercício da liberdade de expressão por parte dos utilizadores de tais meios, garantida pelo artigo 11.º da CDFUE.[65]

[61]Cfr. conclusões *Tele2, cit.*, considerandos 246-248.
[62]Cfr. conclusões *Tele2, cit.*, considerando 262.
[63]Cfr. acórdão *Tele2, cit.*, considerando 112.
[64]Cfr. acórdão *Tele2, cit.*, considerando 125.
[65]Cfr. acórdão *Tele2, cit.*, considerando 101.

De qualquer forma, no entendimento do TJUE a Diretiva 2002/58 não se opõe a que um Estado-Membro adote medidas de conservação seletiva (não generalizada e indiferenciada) de dados de tráfego e de localização para os efeitos da luta contra a delinquência grave, sempre que a conservação esteja limitada ao estritamente necessário quanto *i*) às categorias de dados a conservar-se, *ii*) aos meios de comunicação a que se referem, *iii*) às pessoas afetadas, *iv*) ao período de conservação previsto.[66] Mas então, se a conservação admissível tem de ser seletiva, como é que se delimita uma medida deste tipo quanto ao público e quanto às situações potencialmente afetadas? O TJUE esclarece que a normativa nacional deve basear-se em critérios objetivos que permitam identificar um público cujos dados possam *i*) apresentar uma relação pelo menos indireta com delitos graves, *ii*) contribuir de alguma forma com a luta contra a delinquência grave ou *iii*) prevenir um risco geral para a segurança pública. Tal delimitação pode garantir-se mediante um critério geográfico – isto quando as autoridades nacionais considerem, com base em elementos objetivos, que existe um risco elevado de preparação ou de consecução de tais delitos em uma ou várias zonas geográficas.[67]

Assim, do acórdão *Tele 2* é possível concluir que *i*) a declaração de invalidade das disposições constantes de uma diretiva afeta inelutavelmente o ato legal de transposição das mesmas para a ordem jurídica dos Estados-Membros e *ii*) um Estado-Membro não pode valer-se da Diretiva 2002/58 para impor a manutenção de uma obrigação generalizada e indiferenciada de conservação de dados de tráfego e de localização na sequência da declaração de invalidade da Diretiva 2006/24. Urge, portanto, retirar ilações desta recente decisão do TJUE, tão mais relevante porque, nos Estados-Membros em que a legislação transposta continuou a ser aplicada na sequência da declaração de invalidade da Diretiva 2006/24, muitas condenações penais tiveram por base o acesso a dados conservados de modo potencialmente ilegítimo.

Referências Bibliográficas

BOEHM, F.; COLE, M. **Data Retention after the Judgement of the Court of Justice of the European Union**, 2014. Disponível em: https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

[66]Cfr. acórdão *Tele2, cit.*, considerando 108.
[67]Cfr. acórdão *Tele2, cit.*, considerando 111.

BOEHM, F.; COLE, M. **Data Retention after the Judgement of the Court of Justice of the European Union**, 2014. Disponível em: https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

GABINETE CIBERCRIME DO MINISTÉRIO PÚBLICO. **Nota Prática n.º 7 sobre retenção de dados de tráfego e Lei n.º 32/2008**, 2015. Disponível em: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_retencao_de_dados.pdf

GUERRA, C.; CALVÃO, F. Anotação ao Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014, ***Forum de proteção de dados***, Comissão Nacional de Proteção de Dados, **1**, p. 79–82, jul. 2015.

GUILD, E.; CARRERA, S. The political and judicial life of metadata: Digital Rights Ireland and the trail of the data retention directive. **CEPS Papers in Liberty and Security in Europe**, 65, 2014.

PEERS, S. **The data retention judgment: the CJEU prohibits mass surveillance**, 2014. Disponível em: http://eulawanalysis.blogspot.pt/2014/04/the-data-retention-judgment-cjeu.html

VAINIO, N.; MIETTINEN, S. Telecommunications data retention after *Digital Rights Ireland* : legislative and judicial reactions in the Member States. **International Journal of Law and Information Technology**, v. 23, n. 3, p. 290–309, set. 2015.

WHITE, M. **The new Opinion on data retention: does it protect the right to privacy?**, 2016. Disponível em: http://eulawanalysis.blogspot.pt/2016/07/the-new-opinion-on-data-retention-does.html