TRIBUNAL DE JUSTIÇA
DA UNIÃO EUROPEIA

DIREÇÃO DA INVESTIGAÇÃO
E DOCUMENTAÇÃO

Ficha temática

PROTEÇÃO DOS DADOS PESSOAIS

O direito à proteção dos dados pessoais é um direito fundamental cujo respeito é um importante objetivo para a União Europeia.

O referido direito está consagrado na Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta») que dispõe no seu artigo 8.°:

«1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.»

Este direito fundamental está além disso estreitamente relacionado com o direito ao respeito da vida privada consagrado no artigo 7.° da Carta.

O direito à proteção dos dados pessoais também está previsto no artigo 16.°, n.° 1, do Tratado sobre o Funcionamento da União Europeia (TFUE), que a este respeito sucedeu ao artigo 286.° CE.

Quanto ao direito derivado, a partir de meados dos anos 90 a Comunidade Europeia dotou-se de diferentes instrumentos destinados a garantir a proteção dos dados pessoais. A Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [1], adotada com base no artigo 100.°-A CE,

[1] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31), versão consolidada em 20 de novembro de 2003, revogada a partir de 25 de maio de 2018 (v. nota 5).

constituía o principal ato jurídico da União nesta matéria. Esta diretiva estabelecia as condições gerais de licitude do tratamento desses dados bem como os direitos das pessoas em causa e previa, nomeadamente, a criação de autoridades independentes de controlo nos Estados-Membros.

Em seguida, a Diretiva 2002/58/CE [2] veio completar a Diretiva 95/46, procedendo à harmonização das disposições da legislação dos Estados-Membros relativas à proteção do direito à vida privada, nomeadamente no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas [3]. Importa notar que o legislador da União prevê proceder a uma reapreciação desta diretiva. A este respeito, a Comissão apresentou, em 10 de janeiro de 2017, uma proposta com vista à substituição desta diretiva por um regulamento relativo à vida privada e às comunicações eletrónicas [4].

Além disso, no âmbito do espaço de liberdade, segurança e justiça (ex-artigos 30.° e 31.° do TUE), a Decisão-Quadro 2008/977/JAI [5] regulamentou (até maio de 2018) a proteção dos dados pessoais no domínio da cooperação judiciária em matéria penal e policial.

Em 2016, a União Europeia procedeu à reforma do quadro jurídico geral nesta matéria. Para o efeito, em 2016, adotou o Regulamento (UE) 2016/679 [6] sobre a proteção de dados (a seguir «RGPD»), que revoga a Diretiva 95/46 e que é aplicável desde 25 de maio de 2018, e a Diretiva (UE) 2016/680 [7] que visa a proteção dos referidos dados em matéria penal, que revoga a Decisão-Quadro 2008/977/JAI, e cujo prazo de transposição pelos Estados-Membros foi fixado em 6 de maio de 2018.

Finalmente, no contexto do seu tratamento pelas instituições e órgãos da União, a proteção dos dados pessoais era, num primeiro momento, assegurada pelo Regulamento (CE) n.° 45/2001 [8]. Este regulamento permitiu nomeadamente a criação, em 2004, da Autoridade Europeia para a Proteção de Dados. Em 2018, a União Europeia dotou-se de um novo quadro jurídico nesta matéria, nomeadamente através da adoção do Regulamento (UE) 2018/1725 [9], que revoga o

---

2 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 «Vida privada e comunicações eletrónicas») (JO 2002, L 201, p. 37), versão consolidada em 19 de dezembro de 2009.

3 A Diretiva 2002/58/CE foi alterada pela 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, e que altera a Diretiva 2002/58/CE (JO 2006, L 105, p. 54). Esta diretiva foi declarada inválida pelo Tribunal de Justiça no acórdão de 8 de abril de 2014, Digital Rights Ireland e Seitlinger e o. (C-293/12 e C-594/12, EU:C:2014:238), pelo facto de esta violar gravemente o direito ao respeito da vida privada e à proteção dos dados pessoais (v. rubrica I.1., intitulada «Conformidade do direito derivado da União com o direito à proteção dos dados pessoais» da presente ficha).

4 Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas) COM/2017/010 final - 2017/03 (COD).

5 Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60), revogada a partir de 6 de maio de 2018 (v. nota 6).

6 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (JO 2016, L 119, p. 1).

7 Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO 2016, L 119, p. 89).

8 Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO 2001, L 8, p. 1).

9 Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE.

Regulamento n.º 45/2001 e a Decisão 1247/2002/CE [10] e que é aplicável desde 11 de dezembro de 2018. Para conseguir uma abordagem coerente da proteção de dados pessoais em toda a União, este novo regulamento visa alinhar tanto quanto possível as regras na matéria com o regime estabelecido pelo RGPD.

[10] Decisão n.°°1247/2002/CE do Parlamento Europeu, do Conselho e da Comissão, de 1 de julho de 2002, relativa ao estatuto e às condições gerais de exercício de funções da autoridade europeia para a proteção de dados (JO 2002, L 183, p. 1).

ÍNDICE

I. Direito à proteção dos dados pessoais reconhecido pela Carta dos Direitos Fundamentais da União Europeia 5
1. Conformidade do direito derivado da União com o direito à proteção dos dados pessoais 5
2. Respeito do direito à proteção dos dados pessoais na aplicação do direito da União 9
II. Tratamento dos dados pessoais na aceção da regulamentação geral na matéria 10
1. Tratamento de dados pessoais excluídos do âmbito de aplicação da Diretiva 95/46 10
2. Conceito de «dados pessoais» 13
3. Conceito de «tratamento de dados pessoais» 15
4. Conceito de «ficheiro de dados pessoais» 20
5. Conceito de «responsável pelo tratamento de dados pessoais» 21
6. Requisitos de licitude de um tratamento de dados pessoais 23
III. Tratamento de dados pessoais na aceção da Diretiva 2002/58/CE 33
IV. Transferência dos dados pessoais para países terceiros 39
V. Proteção dos dados pessoais na Internet 47
1. Direito de oposição ao tratamento dos dados pessoais («direito a ser esquecido») 47
2. Tratamento dos dados pessoais e direitos de propriedade intelectual 48
3. Supressão de referências a dados pessoais 52
4. Consentimento do utilizador de um sítio Internet para o armazenamento de informações ou para o acesso a informações através de *cookies* 56
VI. Autoridades nacionais de controlo 57
1. Alcance da exigência de independência 57
2. Determinação do direito aplicável e da autoridade de controlo competente 60
3. Poderes das autoridades nacionais de controlo 61
VII. Aplicação territorial da legislação europeia 65
VIII. Direito de acesso do público aos documentos das instituições da União Europeia e proteção dos dados pessoais 66

I. Direito à proteção dos dados pessoais reconhecido pela Carta dos Direitos Fundamentais da União Europeia

1. Conformidade do direito derivado da União com o direito à proteção dos dados pessoais

Acórdão de 9 de novembro de 2010 (Grande Secção), Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662) [11]

Neste processo, os litígios nos processos principais opunham agricultores ao Land Hessen, a propósito da publicação no sítio Internet da Bundesanstalt für Landwirtschaft und Ernährung (Serviço Federal para a Agricultura e a Alimentação) dos dados pessoais desses agricultores enquanto beneficiários de fundos provenientes do Fundo Europeu Agrícola de Garantia (FEAGA) e do Fundo Europeu Agrícola de Desenvolvimento Rural (FEADER). Os referidos agricultores opuseram-se a esta publicação, alegando, em especial, que esta não era justificada por um interesse público preponderante. O Land Hessen considerava, por seu lado, que a publicação dos referidos dados resultava dos Regulamentos (CE) n.os 1290/2005 [12] e 259/2008 [13], que regem o financiamento da política agrícola comum e impõem a publicação de informações relativas a pessoas singulares beneficiárias do FEAGA e do FEADER.

Foi neste contexto que o Verwaltungsgericht Wiesbaden (Tribunal Administrativo de Wiesbaden, Alemanha) submeteu ao Tribunal várias questões sobre a validade de certas disposições do Regulamento n.º 1290/2005 e do Regulamento n.º 259/2008, que impõem que essas informações sejam colocadas à disposição do público, nomeadamente através de sítios Internet explorados pelos serviços nacionais.

No que respeita à adequação entre o direito à proteção dos dados pessoais reconhecido pela Carta e a transparência em matéria de fundos europeus, o Tribunal salientou que a publicação num sítio Internet de dados nominativos relativos aos beneficiários dos fundos e aos montantes recebidos por estes constitui, em razão do livre acesso por terceiros ao referido sítio, uma violação do direito dos beneficiários em causa ao respeito da sua vida privada, em geral, e à proteção dos seus dados pessoais, em particular (n.os 56 a 64).

Para ser justificada, essa ingerência deve ser prevista por lei, respeitar o conteúdo essencial desses direitos e, em aplicação do princípio da proporcionalidade, ser necessária e responder efetivamente a objetivos de interesse geral reconhecidos pela União, devendo as derrogações e limitações a estes direitos ocorrer na estrita medida do necessário. Neste contexto, o Tribunal considerou que embora numa sociedade democrática os contribuintes tenham o direito de ser

[11] Este acórdão foi apresentado no Relatório Anual de 2010, p. 11.

[12] Regulamento (CE) n.º 1290/2005 do Conselho, de 21 de junho de 2005, relativo ao financiamento da política agrícola comum (JO 2005, L 209, p. 1), revogado pelo Regulamento (UE) n.º 1306/2013 do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativo ao financiamento, à gestão e ao acompanhamento da Política Agrícola Comum (JO 2013, L 347, p. 549).

[13] Regulamento (CE) n.º 259/2008 da Comissão, de 18 de março de 2008, que estabelece as regras de execução do Regulamento (CE) n.º 1290/2005 do Conselho no que respeita à publicação de informação sobre os beneficiários de fundos provenientes do FEAGA e do Feader (JO 2008, L 76, p. 28), revogado pelo Regulamento de Execução (UE) n.º 908/2014 da Comissão, de 6 de agosto de 2014, que estabelece as normas de execução do Regulamento (UE) n.º 1306/2013 do Parlamento Europeu e do Conselho no que diz respeito aos organismos pagadores e outros organismos, gestão financeira, apuramento das contas, controlos, garantias e transparência (JO 2014, L 255, p. 59).

informados sobre a utilização dos fundos públicos, não é menos verdade que o Conselho e a Comissão estavam obrigados a proceder a uma ponderação equilibrada dos interesses em causa, o que implicava, antes da adoção das disposições impugnadas, verificar se a publicação destes dados pelo Estado-Membro num sítio Internet único não ultrapassava o necessário para a realização dos objetivos legítimos prosseguidos (n.os 77, 79, 85 e 86).

Assim, o Tribunal declarou inválidas certas disposições do Regulamento n.º 1290/2005, bem como o Regulamento n.º 259/2008 na totalidade, na medida em que, relativamente às pessoas singulares beneficiárias de ajudas do FEAGA e do Feader, essas disposições impõem a publicação de dados pessoais relativos a qualquer beneficiário, sem proceder a distinções de acordo com critérios pertinentes, como por exemplo os períodos durante os quais receberam essas ajudas, a sua frequência ou ainda o tipo ou a importância das mesmas (n.º 92 e disp. 1). No entanto, o Tribunal não anulou os efeitos da publicação das listas dos beneficiários de tais auxílios efetuada pelas autoridades nacionais durante o período anterior à data da prolação do acórdão (n.º 94 e disp. 2).

Acórdão de 17 de outubro de 2013, Schwarz (C-291/12, EU:C:2013:670)

M. Schwarz tinha solicitado a emissão de um passaporte na Stadt Bochum (Alemanha), tendo-se recusado, nessa ocasião, a autorizar a recolha das suas impressões digitais. Como a Stadt Bochum indeferiu o seu pedido, M. Scharwz interpôs recurso no Verwaltungsgericht Gelsenkirchen (tribunal administrativo de Gelsenkirchen, Alemanha) para que este município fosse obrigado a emitir o seu passaporte sem proceder à recolha das suas impressões digitais. Naquele órgão jurisdicional, M. Schwarz contestava a validade do Regulamento (CE) n.º 2252/2004 [14], que instituiu a obrigação de recolha das impressões digitais dos requerentes de passaportes, alegando, nomeadamente, que esse regulamento violava o direito à proteção dos dados pessoais e o direito ao respeito da vida privada.

Neste contexto, o Verwaltungsgericht Gelsenkirchen submeteu uma questão prejudicial ao Tribunal, com vista a saber se, na medida em que obriga o requerente de um passaporte a fornecer as suas impressões digitais e prevê a sua conservação nos passaportes, o referido regulamento é válido, nomeadamente à luz da Carta.

O Tribunal respondeu afirmativamente, declarando que, embora a recolha e a conservação de impressões digitais pelas autoridades nacionais, regulada no artigo 1.º, n.º 2, do Regulamento n.º 2252/2004, constituam um ato lesivo dos direitos ao respeito da vida privada e à proteção dos dados pessoais, esta violação é justificada pelo objetivo de proteção dos passaportes contra a sua utilização fraudulenta.

Em primeiro lugar, a referida restrição, prevista por lei, prossegue um objetivo de interesse geral reconhecido pela União, na medida em que se destina a impedir, designadamente, a entrada ilegal de pessoas no território da União (n.os 35 a 38). Em seguida, a recolha e a conservação de impressões digitais são aptas a alcançar esse objetivo. Com efeito, por um lado, embora o método de verificação da identidade por meio de impressões digitais não seja totalmente fiável,

[14] Regulamento (CE) n.º 2252/2004 do Conselho, de 13 de dezembro de 2004, que estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros (JO 2004, L 385, p. 1), na redação que lhe foi dada pelo Regulamento (CE) n.º 444/2009 do Parlamento Europeu e do Conselho, de 6 de maio de 2009 (JO 2009, L 142, p. 1).

reduz consideravelmente o risco de aceitação de pessoas não autorizadas. Por outro lado, a falta de concordância das impressões digitais do detentor do passaporte com os dados integrados nesse documento não significa que seja automaticamente recusada à pessoa em causa a entrada no território da União, mas terá como única consequência desencadear um controlo aprofundado destinado a comprovar definitivamente a identidade dessa pessoa (n.os 42 a 45).

Finalmente, quanto ao caráter necessário desse tratamento, não foi dado conhecimento ao Tribunal de medidas suficientemente eficazes, mas que lesem de forma menos gravosa os direitos reconhecidos pelos artigos 7.° e 8.° da Carta do que as medidas resultantes do método baseado nas impressões digitais (n.° 53). O artigo 1.°, n.° 2, do Regulamento n.° 2252/2004 não implica tratamentos das impressões digitais recolhidas que vão além do necessário para a realização do referido objetivo. Com efeito, o referido regulamento indica expressamente que as impressões digitais só podem ser utilizadas com o objetivo de verificar a autenticidade do passaporte e a identidade do seu titular. Além disso, o artigo 1.°, n.° 2, do regulamento garante uma proteção contra o risco de leitura dos dados que contenham impressões digitais por pessoas não autorizadas e só prevê a conservação das impressões digitais no próprio passaporte, o qual continua a ser propriedade exclusiva do seu titular (n.os 54 a 57, 60 e 63).

Acórdão de 8 de abril de 2014 (Grande Secção), Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238) [15]

O presente acórdão tem origem nos pedidos de apreciação da validade da Diretiva 2006/24/CE relativa à conservação de dados, no que respeita ao direito fundamental ao respeito da vida privada e à proteção dos dados pessoais, suscitados no âmbito de litígios nacionais em tribunais irlandeses e austríacos. No processo C-293/12, a High Court (Supremo Tribunal, Irlanda) foi chamada a conhecer de um litígio que opunha a Digital Rights às autoridades irlandesas a respeito da legalidade de medidas nacionais relativas à conservação de dados relativos a comunicações eletrónicas. No processo C-594/12, o Verfassungsgerichtshof (Tribunal Constitucional, Áustria) foi chamado a conhecer de vários recursos em matéria constitucional nos quais se pedia a anulação da disposição nacional que transpunha a Diretiva 2006/24 para o direito austríaco.

Através dos seus pedidos de decisões prejudiciais, os órgãos jurisdicionais irlandeses e austríacos interrogaram o Tribunal sobre a validade da Diretiva 2006/24 à luz dos artigos 7.°, 8.° e 11.° da Carta. Mais precisamente, esses órgãos jurisdicionais nacionais perguntaram ao Tribunal se a obrigação que, por força da referida diretiva, incumbe aos prestadores de serviços de comunicações eletrónicas acessíveis ao público ou de redes públicas de comunicações, de conservar durante um certo período dados relativos à vida privada de uma pessoa e às suas comunicações e de permitir o acesso das autoridades nacionais competentes a esses dados, constituía uma ingerência injustificada nos referidos direitos fundamentais. Os tipos de dados em causa são, designadamente, os dados necessários para encontrar e identificar a fonte e o destino de uma comunicação, para determinar a data, a hora, a duração e o tipo de comunicação, o equipamento de comunicação dos utilizadores, bem como para localizar o equipamento de comunicação móvel, entre os quais figuram, designadamente, o nome e o

[15] Este acórdão foi apresentado no Relatório Anual de 2014, p. 60.

endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário e também um endereço IP para os serviços Internet. Estes dados permitem, designadamente, saber qual é a pessoa com quem um assinante ou um utilizador registado comunicou, e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Além disso, permitem saber com que frequência o assinante ou o utilizador registado comunicam com certas pessoas, durante um certo período.

O Tribunal começou por declarar que, ao impor tais obrigações a estes fornecedores, as disposições da Diretiva 2006/24 eram constitutivas de uma ingerência particularmente grave nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais garantidos pelos artigos 7.° e 8.° da Carta. Neste contexto, o Tribunal declarou que essa ingerência podia ser justificada pela prossecução de um objetivo de interesse geral, como a luta contra a criminalidade organizada. A este respeito, o Tribunal salientou, em primeiro lugar, que a conservação dos dados imposta pela diretiva não era suscetível de violar o conteúdo essencial dos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais, na medida em que não permitia tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal, e previa que os prestadores de serviços ou de redes deviam respeitar certos princípios de proteção e de segurança dos dados. Em segundo lugar, o Tribunal observou que a conservação dos dados e a sua transmissão às autoridades nacionais competentes correspondia efetivamente a um objetivo de interesse geral, concretamente a luta contra a criminalidade grave, bem como, em última análise, a segurança pública (n.os 38 a 44).

No entanto, o Tribunal considerou que, ao adotar a diretiva relativa à conservação de dados, o legislador da União tinha excedido os limites impostos pelo respeito do princípio da proporcionalidade. Por conseguinte, declarou a diretiva inválida, tendo considerado que a ingerência de grande amplitude e de particular gravidade nos direitos fundamentais que a referida diretiva impunha não era suficientemente enquadrada de forma a garantir que se limitava ao estritamente necessário (n.° 65). A Diretiva 2006/24 abrangia efetivamente de maneira geral todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada nenhuma distinção, limitação ou exceção com base no objetivo de luta contra as infrações graves (n.os 57 a 59). Por outro lado, a diretiva não previa nenhum critério objetivo que permitisse garantir que as autoridades nacionais competentes apenas tinham acesso aos dados e apenas podiam utilizá-los para prevenir, detetar ou agir penalmente contra infrações suscetíveis de serem consideradas suficientemente graves para justificar tal ingerência, sendo que também não previa as condições materiais e processuais desse acesso ou utilização (n.os 60 a 62). Por último, relativamente à duração do período de conservação dos dados, a diretiva impunha um prazo de, pelo menos, seis meses, sem proceder a qualquer distinção entre as categorias de dados em função das pessoas em causa ou da eventual utilidade dos dados relativamente ao objetivo prosseguido (n.os 63 e 64).

Por outro lado, no que respeita às exigências decorrentes do artigo 8.°, n.° 3, da Carta, o Tribunal declarou que a Diretiva 2006/24 não previa garantias suficientes que permitissem assegurar uma proteção eficaz dos dados contra os riscos de abuso e contra o acesso e utilização ilícitos dos dados, sendo que também não impunha que os mesmos fossem conservados no território da União.

Por conseguinte, a referida diretiva não garantia plenamente o controlo do respeito das exigências de proteção e de segurança por uma autoridade independente, apesar de tal ser expressamente exigido pela Carta (n.os 66 a 68).

2. Respeito do direito à proteção dos dados pessoais na aplicação do direito da União

Acórdão de 21 de dezembro de 2016 (Grande Secção), Tele2 Sverige (processos apensos C-203/15 e C-698/15, EU:C:2016:970) [16]

Na sequência do acórdão Digital Rights Ireland e Seitlinger e o., que declarou inválida a Diretiva 2006/24 (v. *supra*), o Tribunal foi chamado a conhecer de dois processos que tinham por objeto a obrigação geral aplicável aos prestadores de serviços de comunicações eletrónicas na Suécia e no Reino Unido de conservar os dados relativos às referidas comunicações e cuja conservação estava prevista pela diretiva declarada inválida.

No dia seguinte ao da prolação do acórdão Digital Rights Ireland e Seitlinger e o., a empresa de telecomunicações Tele2 Sverige notificou à autoridade sueca de supervisão dos correios e telecomunicações a sua decisão de deixar de proceder à conservação dos dados bem como a sua intenção de apagar os dados já registados (processo C-203/15). Com efeito, o direito sueco obrigava os prestadores de serviços de comunicações eletrónicas a conservar, de forma sistemática, contínua e sem nenhuma exceção, todos os dados relativos ao tráfego e dados de localização de todos os seus assinantes e utilizadores registados relativos a todos os meios de comunicação eletrónica. No processo C-698/15, três pessoas impugnaram o regime britânico de conservação de dados que permitia ao Ministro do Interior obrigar os operadores públicos de telecomunicações a conservar todos os dados relativos a comunicações por um período máximo de doze meses, estando todavia excluída a conservação do conteúdo de tais comunicações.

O Kammarrätten i Stockholm (Tribunal Administrativo de Recurso de Estocolmo, Suécia) e a Court of Appeal (England & Wales) (Civil Division) (Secção Cível do Tribunal de Recurso de Inglaterra e do País de Gales, Reino Unido)] convidaram o Tribunal a pronunciar-se sobre a interpretação do artigo 15.°, n.° 1, da Diretiva 2002/58, dita «Privacidade e comunicações eletrónicas», que permite aos Estados-Membros introduzir certas exceções à obrigação, prevista nessa diretiva, de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados de tráfego.

No seu acórdão, o Tribunal começou por declarar que o 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, se opõe a uma regulamentação nacional, como a sueca, 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. Segundo o Tribunal, tal regulamentação excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática,

[16] Este acórdão foi apresentado no Relatório Anual de 2016, p. 62.

como exige o referido artigo 15.°, n.° 1, lido à luz dos artigos acima referidos da Carta (n.os 99 a 105, 107, 112 e disp. 1).

Esta disposição, lida à luz desses mesmos artigos da Carta, também se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar esse acesso, no âmbito da luta contra a criminalidade, apenas à luta contra a criminalidade grave, sem submeter o referido acesso a fiscalização prévia por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados no território da União (n.os 118 a 122, 125 e disp. 2).

O Tribunal considerou em contrapartida que o artigo 15.°, n.° 1, da Diretiva 2002/58 não se opõe a uma regulamentação que permite, a título preventivo, com vista à luta contra a criminalidade grave, a conservação seletiva de dados desta natureza, desde que a sua conservação seja limitada ao estritamente necessário no que se refere às categorias de dados abrangidas, aos equipamentos de comunicação visados, às pessoas em causa e à duração de conservação fixada. Para cumprir esses requisitos, esta regulamentação nacional deve, em primeiro lugar, prever normas claras e precisas que permitam proteger eficazmente os dados contra os riscos de abuso. Deve, em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida de conservação dos dados, a título preventivo, garantindo assim que essa medida se limita ao estritamente necessário. Em segundo lugar, no que se refere às condições materiais a que deve obedecer a regulamentação nacional, de modo a assegurar que se limita ao estritamente necessário, a conservação dos dados deve sempre responder a critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido. Em especial, tais condições devem revelar-se, na prática, suscetíveis de limitar efetivamente o alcance da medida e, consequentemente, o público afetado. No que se refere a esta delimitação, a regulamentação nacional deve basear-se em elementos objetivos que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, de contribuir, seja de que maneira for, para a luta contra a criminalidade grave ou de prevenir um risco grave para a segurança pública (n.os 108 a 111).

II. Tratamento dos dados pessoais na aceção da regulamentação geral na matéria

1. Tratamento de dados pessoais excluídos do âmbito de aplicação da Diretiva 95/46

Acórdão de 30 de maio de 2006 (Grande Secção), Parlamento/Conselho (C-317/04 e C-318/04, EU:C:2006:346)

Após os ataques terroristas de 11 de setembro de 2001, os Estados Unidos adotaram uma legislação que dispunha que as transportadoras aéreas que assegurassem ligações com destino ao território dos Estados Unidos ou partida desse território, ou que por ele passassem, eram

obrigadas a fornecer às autoridades aduaneiras americanas um acesso eletrónico aos dados contidos nos seus sistemas automáticos de reserva e de controlo das partidas, denominados «Passenger Name Records» (a seguir «PNR»).

Considerando que estas disposições podiam ser contrárias à legislação europeia e às legislações dos Estados-Membros em matéria de proteção dos dados, a Comissão iniciou negociações com as autoridades americanas. Na sequência dessas negociações, em 14 de maio de 2004, a Comissão adotou a Decisão 2004/535/CE [17], que declarava que o Serviço das Alfândegas e Proteção das Fronteiras dos Estados Unidos (United States Bureau of Customs and Border Protection, a seguir «CBP») assegurava um nível adequado de proteção dos dados dos PNR transferidos a partir da Comunidade (a seguir «decisão de adequação»). Em seguida, em 17 de maio de 2004, o Conselho adotou a Decisão 2004/496/CE [18] que aprovava a celebração de um acordo entre a Comunidade Europeia e os Estados Unidos da América sobre o tratamento e a transferência para o CBP dos dados PNR por parte das transportadoras aéreas com sede no território dos Estados-Membros da Comunidade.

O Parlamento Europeu pediu ao Tribunal que anulasse as duas decisões acima referidas, alegando, nomeadamente, que a decisão de adequação tinha sido adotada *ultra vires*, que o artigo 95.º CE (atual artigo 114.º TFUE) não era uma base jurídica adequada para a decisão de aprovação da celebração do Acordo e que em ambos os casos havia uma violação dos direitos fundamentais.

No que respeita à decisão de adequação, o Tribunal começou por examinar se a Comissão podia validamente adotar a sua decisão com fundamento na Diretiva 95/46. Neste contexto, constatou que decorria da decisão de adequação que a transferência dos dados PNR para o CBP constituía um tratamento que tinha por objeto a segurança pública e as atividades do Estado no domínio do direito penal. Segundo o Tribunal, embora os dados PNR fossem inicialmente recolhidos pelas companhias aéreas no âmbito de uma atividade abrangida pelo direito da União, a saber, a venda de um bilhete de avião que confere o direito a uma prestação de serviços, o tratamento dos dados que era tomado em conta na decisão de adequação era de natureza completamente diferente. Com efeito, esta decisão não visava um tratamento de dados necessário para a realização de uma prestação de serviços, mas um tratamento de dados considerado necessário para salvaguarda da segurança pública e para fins repressivos (n.os 56 e 57).

A este respeito, o Tribunal considerou que o facto de os dados PNR terem sido recolhidos por operadores privados para fins comerciais e de serem estes últimos a organizar a sua transferência para um Estado terceiro não se opunha a que essa transferência fosse considerada um tratamento de dados excluído do âmbito de aplicação da diretiva. Com efeito, essa transferência integrava-se num quadro instituído pelos poderes públicos e que visava a segurança pública. Por conseguinte, o Tribunal concluiu que a decisão de adequação não era abrangida pelo âmbito de aplicação da diretiva, uma vez que dizia respeito a um tratamento de

[17] Decisão 2004/535/CE da Comissão, de 14 de maio de 2004, sobre o nível de proteção adequado dos dados pessoais contidos nos Passenger Name Record transferidos para o Bureau of Customs and Border Protection dos Estados Unidos (JO 2004, L 235, p. 11).

[18] Decisão 2004/496/CE do Conselho, de 17 de maio de 2004, relativa à celebração de um acordo entre a Comunidade Europeia e os Estados Unidos da América sobre o tratamento e a transferência de dados contidos nos registos de identificação dos passageiros (PNR) por parte das transportadoras aéreas para o Serviço das Alfândegas e Proteção das Fronteiras do Departamento de Segurança Interna dos Estados Unidos (JO 2004, L 183, p. 83, e retificativo JO 2005, L 255, p. 168).

dados pessoais que estava excluído da mesma. Por conseguinte, o Tribunal anulou a decisão de adequação (n.os 58 e 59).

No que se refere à decisão do Conselho, o Tribunal declarou que o artigo 95.° CE, lido em conjugação com o artigo 25.° da Diretiva 95/46, não é suscetível de servir de base à competência da Comunidade para celebrar o acordo em questão com os Estados Unidos. Com efeito, este acordo tinha em vista a mesma transferência de dados que a decisão de adequação e, portanto, tratamentos de dados que estavam excluídos do âmbito de aplicação da diretiva. Por conseguinte, o Tribunal anulou a decisão do Conselho que aprovou a celebração do acordo (n.os 67 a 69).

Acórdão de 11 de dezembro de 2014, Ryneš (C-212/13, EU:C:2014:2428)

Em resposta a agressões repetidas, F. Ryneš instalou em sua casa uma câmara de vigilância. Após um novo ataque à sua casa, os registos da referida câmara permitiram identificar dois suspeitos, contra os quais foram instaurados processos-crime. Tendo um dos suspeitos contestado a legalidade do tratamento dos dados registados pela câmara de vigilância perante o Instituto Checo para a proteção dos dados pessoais, este último tinha constatado que F. Ryneš tinha violado as regras em matéria de proteção dos dados pessoais e aplicado uma coima a este último.

Chamado a conhecer de um recurso interposto por F. Ryneš contra uma decisão do Městský soud v Praze (Tribunal da Comarca de Praga, República Checa) que tinha confirmado a decisão do Instituto, o Nejvyšší správní soud (Supremo Tribunal Administrativo) perguntou ao Tribunal de Justiça se a gravação vídeo efetuada por F. Ryneš para proteger a sua vida, a sua saúde e os seus bens constituía um tratamento de dados não abrangido pela Diretiva 95/46 pelo facto de o registo ter sido efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, na aceção do artigo 3.°, n.° 2, segundo travessão, da referida diretiva.

O Tribunal declarou que a exploração de um sistema de câmara, que origina uma gravação vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família, para proteger os bens, a saúde e a vida dos proprietários dessa casa, e que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção desta disposição (n.° 35 e disp.).

A este respeito, o Tribunal recordou que a proteção do direito fundamental ao respeito da vida privada, garantido pelo artigo 7.° da Carta, exige que as derrogações à proteção dos dados pessoais e as respetivas limitações ocorram na estrita medida do necessário. Na medida em que as disposições da Diretiva 95/46, que regulam o tratamento de dados pessoais suscetíveis de pôr em causa as liberdades fundamentais, em especial o direito à vida privada, devem, necessariamente, ser interpretadas à luz dos direitos fundamentais que estão consagrados na referida Carta, a derrogação prevista no artigo 3.°, n.° 2, segundo travessão, desta diretiva deve ser objeto de interpretação estrita (n.os 27 a 29). Além disso, a própria letra desta disposição exclui do âmbito de aplicação da Diretiva 95/46 o tratamento de dados efetuado no exercício de atividades «exclusivamente» pessoais ou domésticas. Ora, uma vez que a videovigilância se estende, ainda que parcialmente, ao espaço público e, por esse motivo, se dirige para fora da

esfera privada da pessoa que procede ao tratamento de dados por esse meio, não pode ser considerada uma atividade exclusivamente «pessoal ou doméstica», na aceção da referida disposição (n.os 30, 31 e 33).

2. Conceito de «dados pessoais»

Acórdão de 19 de outubro de 2016, Breyer (C-582/14, EU:C:2016:779) [19]

P. Breyer tinha intentado uma ação nos tribunais cíveis alemães com vista a que a República Federal da Alemanha fosse proibida de conservar ou mandar conservar por terceiros dados informáticos que eram transmitidos após o termo de cada consulta dos sítios Internet dos serviços federais alemães. Com efeito, a fim de se proteger de ataques e de permitir ações penais contra «piratas», o prestador de serviços de meios de comunicação em linha dos serviços federais alemães gravava dados constituídos por um endereço IP «dinâmico» — um endereço IP que muda por ocasião de cada nova ligação a Internet – bem como a data e a hora da sessão de consulta do sítio. Contrariamente aos endereços IP estáticos, os endereços IP dinâmicos não permitem fazer a ligação *a priori,* através de ficheiros acessíveis ao público, entre um determinado computador e a ligação física à rede utilizada pelo fornecedor de acesso à Internet. Os dados registados, por si só, não ofereciam ao fornecedor de serviços de comunicação social em linha a possibilidade de identificar o utilizador. Em contrapartida, por sua vez, o fornecedor de acesso à Internet dispunha de informações suplementares que caso fossem combinadas com esse endereço IP permitiam identificar o referido utilizador.

Neste contexto, o Bundesgerichtshof (Tribunal Federal de Justiça, Alemanha), chamado a pronunciar-se em sede de um recurso de «Revision», interrogou o Tribunal sobre a questão de saber se um endereço IP que é registado por um prestador de serviços de meios de comunicação em linha quando acede ao seu sítio Internet constitui um dado pessoal.

O Tribunal começou por observar que, para que um dado possa ser qualificado de «dado pessoal», na aceção do artigo 2.°, alínea a), da Diretiva 95/46, não é necessário que todas as informações que permitem identificar a pessoa em causa estejam na posse de uma única pessoa. O facto de as informações suplementares necessárias para identificar o utilizador de um sítio Internet não serem detidas pelo prestador de serviços de meios de comunicação em linha, mas pelo fornecedor de acesso à Internet desse utilizador, não parece, assim, suscetível de excluir que os endereços IP dinâmicos registados pelo prestador de serviços de meios de comunicação em linha constituam, para este, dados pessoais na aceção do artigo 2.°, alínea a), da Diretiva 95/46 (n.os 43 e 44).

Por conseguinte, o Tribunal constatou que um IP dinâmico, registado por um prestador de serviços de meios de comunicação em linha quando alguém consulta um sítio Internet que esse prestador disponibiliza ao público, constitui, relativamente a esse prestador, um dado pessoal na aceção do artigo 2.°, alínea a), da Diretiva 95/46/CE, quando este disponha de meios legais que lhe permitam identificar a pessoa em causa graças às informações suplementares de que o fornecedor de acesso à Internet dessa pessoa dispõe (n.° 49 e disp. 1).

[19] Este acórdão foi apresentado no Relatório Anual de 2016, p. 61.

Acórdão de 20 de dezembro de 2017, Nowak (C-434/16, EU:C:2017:994)

P. Nowak, um contabilista estagiário, reprovou no exame organizado pela Câmara irlandesa dos técnicos oficiais de contas. P. Nowak tinha apresentado um pedido de acesso a todos os dados pessoais que lhe diziam respeito detidos pela Câmara dos técnicos oficiais de contas, ao abrigo do artigo 4.° da lei de proteção de dados. Esta última tinha comunicado a P. Nowak alguns documentos, mas recusou-se a entregar-lhe a cópia do seu exame pelo facto de a mesma não conter dados pessoais relativos ao requerente, na aceção da lei relativa à proteção dos dados.

Na medida em que, pelos mesmos motivos, o Comissário para a proteção dos dados também não deferiu o seu pedido de acesso, P. Nowak intentou uma ação nos órgãos jurisdicionais nacionais. A Supreme Court (Supremo Tribunal, Irlanda), chamada a conhecer de um recurso interposto por P. Nowak, submeteu ao Tribunal de Justiça a questão de saber se o artigo 2.°, alínea a), da Diretiva 95/46 deve ser interpretado no sentido de que, em condições como as que estão em causa no processo principal, as respostas escritas dadas por um candidato durante um exame profissional e as eventuais anotações do examinador com elas relacionadas constituem dados pessoais na aceção dessa disposição.

Em primeiro lugar, o Tribunal considerou que, para que um dado possa ser qualificado de «dado pessoal», na aceção do artigo 2.°, alínea a), da Diretiva 95/46, não é necessário que todas as informações que permitem identificar a pessoa em causa estejam na posse de uma única pessoa. Por outro lado, na hipótese de o examinador não conhecer a identidade do candidato aquando da notação das respostas dadas por este num exame, a entidade que organiza o exame, no caso em apreço, a Câmara dos técnicos oficiais de contas, dispõe, em contrapartida, das informações necessárias que lhe permitem identificar o candidato sem qualquer dificuldade ou dúvida a partir do seu número de identificação inscrito na folha de respostas do exame ou na capa da mesma, e, assim, identificar as suas respostas.

Em segundo lugar, o Tribunal concluiu que as respostas escritas fornecidas por um candidato num exame profissional constituem informações relacionadas com a sua pessoa. Com efeito, o conteúdo dessas respostas reflete o nível de conhecimentos e de competência do candidato num dado domínio, bem como, sendo caso disso, o seu processo de reflexão, o seu julgamento e o seu espírito crítico. Além disso, a recolha das referidas respostas tem como finalidade avaliar as capacidades profissionais do candidato e a sua aptidão para exercer a profissão em causa. Acresce que a utilização dessas informações, que se traduz, designadamente, pela aprovação ou reprovação do candidato no exame em causa, é suscetível de ter um efeito sobre os seus direitos e interesses, na medida em que pode determinar ou influenciar, por exemplo, as possibilidades de esse candidato aceder à profissão ou ao emprego pretendidos. A conclusão de que as respostas escritas dadas por um candidato num exame profissional constituem informações que dizem respeito a esse candidato devido ao seu conteúdo, à sua finalidade e ao seu efeito é válida igualmente quando se trate de um exame com consulta (n.os 31 e 36 a 40).

Em terceiro lugar, no que respeita às anotações do examinador relativas às respostas do candidato, o Tribunal considerou que estas constituem, juntamente com as respostas do candidato no exame, informações sobre esse candidato, uma vez que refletem a opinião ou a apreciação do examinador quanto à prestação individual do candidato no exame e, designadamente, quanto aos seus conhecimentos e às suas competências no domínio em causa. Além disso, as referidas anotações têm precisamente como finalidade documentar a

avaliação da prestação do candidato feita pelo examinador e são suscetíveis de ter efeitos para este último (n.os 42 e 43).

Em quarto lugar, o Tribunal considerou que as respostas escritas dadas por um candidato num exame profissional e as eventuais anotações do examinador com elas relacionadas podem estar sujeitas a uma verificação, designadamente, da respetiva exatidão e da necessidade da sua conservação, na aceção do artigo 6.°, n.° 1, alíneas d) e e), da Diretiva 95/46, e podem ser objeto de uma retificação ou de um apagamento, ao abrigo do seu artigo 12.°, alínea b). O facto de conferir ao candidato um direito de acesso a essas respostas e a essas anotações, nos termos do artigo 12.°, alínea a), desta diretiva, serve o objetivo desta última, que consiste em garantir a proteção do direito à vida privada desse candidato relativamente ao tratamento dos dados que lhe dizem respeito e tal independentemente da questão de saber se o referido candidato dispõe ou não desse direito de acesso, igualmente ao abrigo da legislação nacional aplicável ao procedimento de exame. No entanto, o Tribunal sublinhou que os direitos de acesso e de retificação, ao abrigo do artigo 12.°, alíneas a) e b), da Diretiva 95/46, não são extensivos às questões do exame, que não constituem, enquanto tais, dados pessoais do candidato (n.os 56 e 58).

Tendo em conta estes elementos, o Tribunal concluiu que, em condições como as que estavam em causa no processo principal, as respostas escritas fornecidas por um candidato num exame profissional e as anotações do examinador relativas a essas respostas constituem dados pessoais, na aceção do artigo 2.°, alínea a), da Diretiva 95/46 (n.° 62 e disp.).

3. Conceito de «tratamento de dados pessoais»

Acórdão de 6 de novembro de 2003 (Grande Secção), Lindqvist (C-101/01, EU:C:2003:596)

B. Lindqvist, trabalhadora voluntária numa paróquia da Igreja Protestante na Suécia, criou páginas Internet com o seu computador pessoal nas quais publicou dados pessoais sobre várias pessoas que, como ela, trabalhavam como voluntárias na referida paróquia. B. Lindqvist foi condenada no pagamento de uma coima por ter utilizado dados pessoais no contexto de um tratamento automatizado sem ter previamente procedido à declaração escrita junto da Datainspektion sueca (organismo público para a proteção dos dados transmitidos por via informática), por ter transferido esses dados sem autorização para países terceiros e por ter tratado dados pessoais sensíveis.

No âmbito do recurso interposto por B. Lindqvist desta decisão no Göta hovrätt (tribunal de recurso, Suécia), este último interrogou o Tribunal a título prejudicial com vista a saber, em particular, se B. Lindqvist tinha procedido a um «tratamento de dados pessoais por meios total ou parcialmente automatizados» na aceção da Diretiva 95/46.

O Tribunal declarou que a operação que consiste na referência, numa página da Internet, a várias pessoas e à sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos, constitui um «tratamento de dados pessoais por meios total ou parcialmente automatizados», na aceção desta diretiva (n.° 27 e disp. 1). Com efeito, tal tratamento de dados pessoais, efetuado para o exercício de atividades benévolas ou religiosas, não é abrangido por nenhuma

das exceções ao âmbito de aplicação da diretiva, na medida em que não se integra nem na categoria de atividades que têm por objeto a segurança pública nem na categoria de atividades exclusivamente pessoais ou domésticas que estão fora do âmbito de aplicação da diretiva (n.os 38, 43 a 48 e disp. 2).

Acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, EU:C:2014:317)

Em 2010, um cidadão espanhol apresentou à Agencia Española de Protección de Datos (Agência Espanhola de Proteção de Dados, a seguir «AEPD») uma reclamação contra a La Vanguardia Ediciones SL, editora de um jornal de grande tiragem em Espanha, bem como contra a Google Spain e a Google. Essa pessoa alegava que, quando um internauta inseria o seu nome no motor de busca do grupo Google, a lista de resultados tinha ligações a duas páginas do jornal La Vanguardia, datados de 1998, em que se anunciava uma venda de imóveis em hasta pública realizada na sequência de um arresto com vista à recuperação das suas dívidas. Com esta reclamação, M. Costeja González pedia, por um lado, que se ordenasse ao La Vanguardia que suprimisse ou alterasse as referidas páginas ou que se utilizassem certas ferramentas disponibilizadas pelos motores de busca para proteger esses dados. Por outro lado, pedia que a Google Spain ou a Google Inc. fossem intimadas a suprimir ou a ocultar os seus dados pessoais, para que os mesmos deixassem de ser exibidos nos resultados de pesquisa e de figurar nas ligações do La Vanguardia.

A AEPD tinha indeferido a reclamação contra o La Vanguardia, considerando que as informações em causa tinham sido legalmente publicadas pelo editor, mas, em contrapartida, deferiu-a no que respeita à Google Spain e à Google, tendo requerido a estas duas sociedades que adotassem as medidas necessárias para retirar os dados do seu índice e para impossibilitar o acesso às mesmas no futuro. Tendo as referidas sociedades interposto recurso perante a Audiencia Nacional (Audiência Nacional, Espanha), a fim de obter a anulação da decisão da AEPD, o órgão jurisdicional espanhol apresentou uma série de questões ao Tribunal.

Assim, o Tribunal teve a oportunidade de precisar o conceito de «tratamento de dados pessoais» na Internet em conformidade com a Diretiva 95/46.

O Tribunal declarou, assim, que a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por uma determinada ordem de preferência deve ser qualificada de tratamento de dados pessoais quando essas informações contenham dados pessoais (disp. 1). O Tribunal recordou, além disso, que as operações visadas pela diretiva devem ser qualificadas de tratamento, incluindo quando são exclusivamente relativas a informações já publicadas nos meios de comunicação social. Uma derrogação geral à aplicação da diretiva neste caso teria por efeito esvaziá-la amplamente do seu sentido (n.os 29 e 30).

Acórdão de 10 de julho de 2018 (Grande Secção), Jehovan todistajat (C-25/17, EU:C:2018:551) [20]

A autoridade finlandesa de proteção de dados tinha adotado uma decisão que proibia a Comunidade das Testemunhas de Jeová de recolher ou tratar dados pessoais no contexto da atividade de pregação porta-a-porta efetuada pelos membros dessa comunidade, sem que fossem respeitados os requisitos da legislação finlandesa relativa ao tratamento de dados pessoais. Com efeito, no contexto da atividade de pregação porta-a-porta, os membros desta comunidade tomam notas sobre as visitas a pessoas que nem eles próprios nem a referida comunidade conhecem. Esses dados são recolhidos para memória futura, para poderem ser consultados com vista a uma eventual visita posterior, sem que as pessoas em causa tenham dado o seu consentimento ou tenham disso sido informadas. A este respeito, a Comunidade das Testemunhas de Jeová deu aos seus membros orientações relativas à recolha dessas notas que constavam de, pelo menos, uma das suas publicações consagradas à atividade de pregação.

O Tribunal declarou que nem a recolha de dados pessoais por membros de uma comunidade religiosa no contexto de uma atividade de pregação porta-a-porta nem os posteriores tratamentos desses dados são abrangidos pelas exceções ao âmbito de aplicação da Diretiva 95/46, dado que não constituem tratamentos de dados pessoais efetuados no exercício de atividades referidas no artigo 3.°, n.° 2, primeiro travessão desta diretiva nem tratamentos de dados pessoais efetuados por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas, na aceção do artigo 3.°, n.° 2, segundo travessão da referida diretiva (n.° 51 e disp. 1).

Acórdão de 14 de fevereiro de 2019, Buivids (C-345/17, EU:C:2019:122)

Neste processo, o Tribunal debruçou-se sobre a interpretação, por um lado, do âmbito de aplicação da Diretiva 95/46 e, por outro, sobre o conceito de «tratamento de dados pessoais efetuado para fins exclusivamente jornalísticos», visado no artigo 9.° desta diretiva.

Este acórdão inscreve-se no contexto de um pedido de decisão prejudicial apresentado pelo Supremo Tribunal da Letónia, chamado a pronunciar-se a respeito de um litígio que opunha S. Buivids (a seguir «recorrente») à autoridade nacional de proteção de dados, a propósito de um recurso em que era pedida a declaração de ilegalidade de uma decisão daquela autoridade, nos termos da qual o recorrente tinha violado a legislação nacional em matéria de proteção de dados pessoais ao publicar, num sítio internet, um vídeo, filmado por ele próprio, da sua prestação de declarações nas instalações da esquadra da polícia nacional no contexto de um processo contraordenacional. Assim, e na medida em que duas instâncias inferiores negaram provimento ao seu recurso, o recorrente interpôs recurso de cassação. Perante o órgão jurisdicional de reenvio, o recorrente invocou o seu direito à liberdade de expressão alegando que o vídeo em causa mostrava funcionários da polícia nacional, que têm a qualidade de pessoas públicas, num local acessível ao público e que, por isso, essas pessoas não beneficiam da aplicação das disposições da lei sobre a proteção de dados.

[20] Este acórdão foi apresentado no Relatório Anual de 2018, pp. 87 e 88.

No que respeita, em primeiro lugar, ao âmbito de aplicação da Diretiva 95/46, o Tribunal observou, por um lado, que as imagens dos membros da polícia registadas no vídeo em causa constituem dados pessoais e que, por outro, a gravação vídeo dessas pessoas, guardada na câmara utilizada pelo recorrente, constitui um tratamento de dados pessoais. Assim, o Tribunal acrescentou que o facto de publicar uma gravação vídeo da qual constam dados pessoais num sítio Internet de vídeos que os utilizadores podem visualizar e partilhar constitui um tratamento total ou parcialmente autorizado desses dados. Por outro lado, o Tribunal sublinhou que a referida gravação e respetiva publicação não são abrangidas pelas exceções previstas no âmbito de aplicação da Diretiva 95/46, relativas nomeadamente aos tratamentos pessoais realizados no contexto das atividades que não são abrangidas pelo âmbito de aplicação desta diretiva e aos tratamentos que se inscrevem no contexto do exercício de atividades exclusivamente pessoais ou domésticas. Por conseguinte, o Tribunal concluiu que estão abrangidas pelo âmbito de aplicação desta diretiva a gravação vídeo de agentes da polícia numa esquadra, aquando de uma prestação de declarações, e a publicação do vídeo assim gravado num sítio Internet de vídeos no qual os utilizadores podem carregar, visualizar e partilhar os mesmos (n.os 31, 32, 35, 39, 42, 43 e disp. 1).

Em segundo lugar, no que diz respeito ao alcance do conceito de «tratamento de dados pessoais para fins exclusivamente jornalísticos», o Tribunal começou por recordar que, em aplicação de uma interpretação ampla do conceito de «jornalismo», as exceções e derrogações previstas no artigo 9.° da Diretiva 95/46 são aplicáveis a qualquer pessoa que exerça a atividade de jornalismo. Assim, o Tribunal declarou que o facto de o recorrente não ser jornalista profissional não exclui que a gravação do vídeo em causa e a sua transmissão possam ser qualificadas de «tratamento de dados pessoais para fins exclusivamente jornalísticos». Além disso, o Tribunal sublinhou que as exceções e as derrogações previstas no artigo 9.° da Diretiva 95/46 só devem ser aplicadas na medida em que sejam necessárias para conciliar dois direitos fundamentais, concretamente, o direito à proteção da vida privada e a liberdade de expressão. A este respeito, o Tribunal precisou que não era de excluir que a gravação e a publicação do vídeo em causa, que ocorreram sem que os agentes da polícia que apareciam nesse vídeo tivessem sido informados dessa gravação e das suas finalidades, constituíssem uma ingerência no direito fundamental ao respeito pela vida privada dessas pessoas. Por conseguinte, concluiu que a gravação e a publicação do vídeo em causa, num sítio Internet de vídeos, podem constituir um tratamento de dados pessoais para fins exclusivamente jornalísticos, desde que resulte do vídeo em causa que a referida gravação e que a referida publicação têm por única finalidade a divulgação ao público de informações, opiniões ou ideias, o que incumbe ao órgão jurisdicional de reenvio verificar (n.os 51, 52, 55, 63, 67 e disp. 2).

Acórdão de 22 de junho de 2021 (Grande Secção), Latvijas Republikas Saeima (Pontos de penalização) (C-439/19, EU:C:2021:504)

B é uma pessoa singular a quem foram aplicados pontos de penalização pela prática de uma ou várias infrações rodoviárias. Esses pontos de penalização foram registados pela Ceļu satiksmes drošības direkcija (Direção da Segurança Rodoviária, Letónia) (a seguir «CSDD») no registo nacional de veículos e condutores.

Por força da legislação letã sobre a circulação rodoviária [21], as informações relativas aos pontos de penalização aplicados aos condutores de veículos inscritos nesse registo são acessíveis ao público e são comunicadas pela CSDD a qualquer pessoa que o solicite, sem que esta tenha de demonstrar um interesse específico em obter essas informações, incluindo a operadores económicos para efeitos de reutilização. Interrogando-se sobre a legalidade desta legislação, B interpôs um recurso constitucional perante o Latvijas Republikas Satversmes tiesa (Tribunal Constitucional, Letónia), para que este examinasse a conformidade dessa regulamentação com o direito ao respeito pela vida privada.

O Tribunal Constitucional considerou que deve ter em conta o RGPD no âmbito da sua apreciação deste direito constitucional. Nesta medida, pediu ao Tribunal de Justiça uma clarificação a respeito do alcance de várias disposições do RGPD com o objetivo de determinar a compatibilidade da legislação letã sobre a circulação rodoviária com esse regulamento.

No seu acórdão, proferido em Grande Secção, o Tribunal de Justiça declara que o tratamento de dados pessoais relativos aos pontos de penalização constitui um «tratamento de dados pessoais relativos a condenações penais e a infrações» [22], para o qual o RGPD prevê uma proteção acrescida devido à particular sensibilidade dos dados em causa (n.os 10, 46, 74, 94 e disp. 1).

Neste contexto, observa, a título preliminar, que as informações relativas aos pontos de penalização configuram dados pessoais e que a sua comunicação pela CSDD a terceiros constitui um tratamento abrangido pelo âmbito de aplicação material do RGPD. Com efeito, este âmbito de aplicação é muito amplo e o tratamento em causa não é abrangido pelas exceções à aplicabilidade deste regulamento (n.os 60, 61 e 72).

Assim, por um lado, este tratamento não está abrangido pela exceção relativa à não aplicação do RGPD a um tratamento efetuado no exercício de uma atividade não sujeita à aplicação do direito da União [23]. Deve considerar-se que esta exceção tem por único objetivo excluir do âmbito de aplicação deste regulamento os tratamentos de dados pessoais efetuados pelas autoridades estatais no âmbito de uma atividade que visa preservar a segurança nacional ou de uma atividade que pode ser classificada na mesma categoria. Estas atividades abrangem, em especial, as que tem por objeto proteger as funções essenciais do Estado e os interesses fundamentais da sociedade. Ora, as atividades relacionadas com a segurança rodoviária não prosseguem esse objetivo e não podem, por conseguinte, ser classificadas na categoria das atividades que têm por finalidade a preservação da segurança nacional (n.os 62 e 66 a 68).

Por outro lado, a comunicação de dados pessoais relativos aos pontos de penalização também não constitui um tratamento abrangido pela exceção que prevê a não aplicação do RGPD aos tratamentos de dados pessoais efetuados pelas autoridades competentes em matéria penal [24].

[21] Artigo 141, n.º 2, do Ceļu satiksmes likums (Lei da Circulação Rodoviária), de 1 de outubro de 1997 (Latvijas Vēstnesis, 1997, n.º 274/276).
[22] Artigo 10.º do RGPD.
[23] Artigo 2.º, n.º 2, alínea a), do RGPD.
[24] Artigo 2.º, n.º 2, alínea d), do RGPD.

Com efeito, o Tribunal de Justiça declara que, quando efetua a referida comunicação, não se pode considerar que a CSDD seja essa «autoridade competente» [25] (n.os 69 a 71).

Para determinar se o acesso aos dados pessoais relativos às infrações rodoviárias, como os pontos de penalização, constitui um tratamento de dados pessoais relativos a «infrações» [26], que beneficiam de proteção acrescida, o Tribunal de Justiça declara, baseando-se nomeadamente na génese do RGPD, que este conceito remete exclusivamente para as infrações penais. Todavia, o facto de, no sistema jurídico letão, as infrações rodoviárias serem consideradas infrações administrativas não é determinante para apreciar se essas infrações estão abrangidas pelo conceito de «infração penal», na medida em que se trata de um conceito autónomo do direito da União que exige, em toda a União, uma interpretação autónoma e uniforme. Assim, após ter recordado os três critérios pertinentes para apreciar o caráter penal de uma infração, a saber, a qualificação jurídica da infração no direito interno, a natureza da infração e o grau de severidade da sanção em que incorre, o Tribunal de Justiça considera que as infrações rodoviárias em causa estão abrangidas pelo conceito de «infração» na aceção do RGPD. Quanto aos dois primeiros critérios, o Tribunal de Justiça declara que, mesmo que as infrações não sejam qualificadas como «penais» no direito nacional, tal caráter pode resultar da natureza da infração, nomeadamente da finalidade repressiva prosseguida pela sanção que a infração é suscetível de desencadear. Ora, no caso em apreço, a atribuição de pontos de penalidade por infrações rodoviárias, tal como as outras sanções que a sua prática pode implicar, prosseguem, entre outros, uma finalidade repressiva desse tipo. Quanto ao terceiro critério, o Tribunal observa que só infrações rodoviárias de uma certa gravidade implicam a atribuição de pontos de penalização e que, portanto, essas infrações são suscetíveis de dar lugar a sanções de uma certa gravidade. Além disso, a aplicação desses pontos acresce geralmente à sanção aplicada, e a cumulação destes pontos tem consequências jurídicas que podem mesmo ir até à proibição de conduzir (n.os 77, 80, 85, 87 a 90 e 93).

4. Conceito de «ficheiro de dados pessoais»

Acórdão de 10 de julho de 2018 (Grande Secção), Jehovan todistajat (C-25/17, EU:C:2018:551)

Neste acórdão (ver igualmente a rubrica II.3., intitulada «Conceito de "tratamento de dados pessoais"»), o Tribunal precisou o conceito de «ficheiro», previsto no artigo 2.°, alínea c), da Diretiva 95/46.

Assim, depois de ter recordado que esta diretiva só se aplica a tratamentos manuais de dados pessoais quando os dados tratados estiverem contidos num ficheiro ou a ele forem destinados, o Tribunal declarou que o referido conceito abrange um conjunto de dados pessoais recolhidos no âmbito de uma atividade de pregação porta-a-porta, do qual constem os nomes e os endereços e outras informações relativas às pessoas abordadas, desde que tais dados sejam estruturados segundo critérios específicos que, na prática, permitam encontrá-los facilmente

[25] Artigo 3.°, n.° 7, da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, 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, e que revoga a Decisão Quadro 2008/977/JAI do Conselho (JO 2016, L 119, p. 89).

[26] Artigo 10.° do RGPD.

para utilização posterior. Para que esse conjunto de dados seja abrangido por este conceito, não é necessário que inclua fichas, listas específicas ou outros sistemas de pesquisa (n.° 62 e disp. 2).

5. Conceito de «responsável pelo tratamento de dados pessoais»

Acórdão de 10 de julho de 2018 (Grande Secção), Jehovan todistajat (C-25/17, EU:C:2018:551)

Neste processo (v. igualmente as rubricas II.3. e II.4., intituladas «Conceito de "tratamento de dados pessoais" e «Conceito de "ficheiro de dados pessoais"»), o Tribunal pronunciou-se a respeito da responsabilidade de uma comunidade religiosa relativamente aos tratamentos de dados pessoais efetuados no quadro de uma atividade de pregação porta-a-porta organizada, coordenada e encorajada por esta comunidade.

Assim, o Tribunal considerou que o dever de respeitar as regras de direito da União em matéria de proteção de dados pessoais não pode ser considerado uma ingerência na autonomia organizacional das comunidades religiosas. Concluiu, a este respeito, que o artigo 2.°, alínea d), da Diretiva 95/46, lido à luz do artigo 10.°, n.° 1, da Carta, deve ser interpretado no sentido de que permite considerar uma comunidade religiosa conjuntamente responsável com os seus membros pregadores pelo tratamento de dados pessoais efetuado por estes últimos no âmbito de uma atividade de pregação porta-a-porta organizada, coordenada e promovida por esta comunidade, não sendo necessário que a referida comunidade tenha acesso aos dados, nem que deva ser demonstrado que essa comunidade deu orientações escritas ou instruções a respeito desses tratamentos aos seus membros (n.os 74, 75 e disp. 3).

Acórdão de 5 de junho de 2018 (Grande Secção), Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388) [27]

Na sua qualidade de autoridade de controlo, na aceção do artigo 28.° da Diretiva 95/46, a autoridade alemã de proteção de dados tinha ordenado que uma sociedade alemã, especializada no domínio da educação e que oferecia serviços de formação através de uma página de fãs alojada no sítio da rede social Facebook, desativasse essa sua página de fãs. Com efeito, segundo a referida autoridade, nem esta sociedade nem a Facebook tinham informado os visitantes da referida página de fãs de que esta última recolhia, através de *cookies,* informações pessoais que lhes diziam respeito e que a referida sociedade e a Facebook em seguida tratavam esses dados.

Nesse contexto, o Tribunal precisou o conceito de «responsável pelo tratamento» de dados pessoais. Considerou, a este respeito, que o administrador de uma página de fãs alojada no Facebook, como a sociedade em causa no processo principal, participa, através da sua ação de parametrização (em função, designadamente, da sua audiência alvo, bem como de objetivos de gestão ou de promoção das suas atividades), na determinação das finalidades e dos meios do tratamento dos dados pessoais dos visitantes da sua página de fãs. Logo, segundo o Tribunal,

[27] Este acórdão foi apresentado no Relatório Anual de 2018, pp. 86 e 87.

este administrador deve ser qualificado de responsável na União, conjuntamente com o Facebook Ireland (filial da sociedade americana Facebook na União Europeia), por esse tratamento, na aceção do artigo 2.°, alínea d), da Diretiva 95/46 (n.° 39).

Acórdão de 29 de julho de 2019, Fashion ID (C-40/17, EU:C:2019:629)

Neste processo, o Tribunal teve a ocasião de desenvolver o conceito de «responsável pelo tratamento» relativamente à integração de um «plugin» numa página Internet.

No caso concreto, a Fashion ID, empresa alemã de venda em linha de vestuário de moda, tinha inserido no seu sítio Internet o módulo social «gosto» da rede social Facebook. Esta inserção tinha como consequência que, quando um visitante consultava o sítio Internet da Fashion ID, os dados pessoais desse visitante eram transmitidos à Facebook Ireland. Esta transmissão era efetuada sem que o referido visitante dela estivesse consciente e independentemente do facto de ser membro da rede social Facebook ou de ter clicado no botão «gosto» da Facebook.

A Verbraucherzentrale NRW, associação alemã de utilidade pública de defesa dos interesses dos consumidores, acusa a Fashion ID de ter transmitido à Facebook Ireland dados pessoais pertencentes aos visitantes do seu sítio Internet, por um lado, sem o consentimento destes últimos e, por outro, em violação das obrigações de informação previstas pelas disposições relativas à proteção de dados pessoais. Chamado a conhecer do processo, o Oberlandesgericht Düsseldorf (Tribunal Regional Superior de Düsseldorf, Alemanha) pediu ao Tribunal que procedesse à interpretação de várias disposições da Diretiva 95/46.

O Tribunal constatou, em primeiro lugar, que o administrador de um sítio Internet, como a Fashion ID, pode ser considerado responsável pelo tratamento, na aceção do artigo 2.°, alínea d), da Diretiva 95/46. Essa responsabilidade é, porém, limitada à operação ou ao conjunto de operações de tratamento de dados pessoais cujas finalidades e meios são efetivamente determinados por esse administrador, a saber, a recolha e a comunicação por transmissão dos dados em causa. Em contrapartida, segundo o Tribunal, parece em primeiro lugar ser de excluir que a Fashion ID determine as finalidades e os meios das posteriores operações de tratamento de dados pessoais, efetuadas pela Facebook Ireland após a transmissão destes a esta última, pelo que a Fashion ID não pode ser considerada responsável por essas operações, na aceção desse artigo 2.°, alínea d) (n.ºs 76, 85 e disp. 2).

Além disso, o Tribunal sublinhou que é necessário que, com essas operações de tratamento, o administrador de um sítio Internet e o fornecedor de um módulo social, como a Facebook Ireland, prossigam, cada um deles, um interesse legítimo, na aceção do artigo 7.°, alínea f), da Diretiva 95/46, para que essas operações sejam justificadas a seu respeito (n.° 97 e disp. 3).

Por último, o Tribunal precisou que o consentimento da pessoa em causa, previsto no artigo 2.°, alínea h), e no artigo 7.°, alínea a), da Diretiva 95/46, deve ser obtido pelo administrador de um sítio Internet unicamente no que diz respeito às operações de tratamento de dados pessoais, cujas finalidades e meios são determinados por esse administrador. Em tal situação, a obrigação de informação prevista pelo artigo 10.° desta diretiva impende igualmente sobre o administrador, devendo, no entanto, a informação que este deve fornecer à pessoa em causa

incidir apenas sobre a operação ou o conjunto das operações de tratamento de dados pessoais cujas finalidades e meios são determinados pelo administrador em causa (n.° 106 e disp. 4).

Acórdão de 9 de julho de 2020, Land Hessen, C-272/19, EU:C:2020:535

Um cidadão que tinha apresentado uma petição à Comissão das Petições do Parlamento do *Land* do Hesse (Alemanha) pediu a esta última para aceder aos dados pessoais que lhe diziam respeito e que tinham sido conservados por esta Comissão no âmbito do tratamento da sua petição. O seu pedido baseava-se no RGPD que prevê que o titular dos dados em causa tem direito a que o responsável pelo tratamento lhe conceda o acesso aos dados pessoais que lhe dizem respeito.

O presidente do Parlamento do *Land* do Hesse indeferiu este pedido pelo facto de o procedimento de petição constituir uma missão parlamentar e de o Parlamento não estar sujeito ao RGPD.

O Verwaltungsgericht Wiesbaden (Tribunal Administrativo de Wiesbaden, Alemanha), perante o qual o cidadão interpôs recurso, considera que o direito alemão não concede direito de acesso aos dados pessoais no âmbito de uma petição como a que está em causa neste processo. Contudo, por entender que tal direito de acesso pode decorrer do RGPD, o Verwaltungsgericht decidiu submeter esta questão ao Tribunal de Justiça. Por outro lado, por ter dúvidas sobre a sua própria independência e, por conseguinte, sobre a sua própria qualidade de órgão jurisdicional, autorizado a submeter questões prejudiciais ao Tribunal de Justiça, o Verwaltungsgericht interrogou igualmente o Tribunal de Justiça sobre este aspeto.

No seu acórdão o Tribunal de Justiça respondeu que, na medida em que determina, individualmente ou em conjunto com outros, as finalidades e os meios do tratamento dos dados pessoais, uma Comissão das Petições do Parlamento de um Estado federado de um Estado-Membro deve ser qualificada de «responsável pelo tratamento» na aceção do RGPD [28]. O tratamento de dados pessoais efetuado por tal comissão está assim submetido a este regulamento, designadamente à disposição que confere às pessoas interessadas direito de acesso aos dados pessoais que lhes digam respeito [29].

O Tribunal constata nomeadamente que as atividades da Comissão das Petições do Parlamento do *Land* do Hesse não estão abrangidas por uma exceção prevista no RGPD. Reconhece que tais atividades são de natureza pública e próprias deste *Land*, uma vez que esta comissão contribui indiretamente para a atividade parlamentar, mas salienta que estas atividades são igualmente de natureza tanto política como administrativa. Além disso, não resulta de modo nenhum dos elementos de que o Tribunal dispõe que estas atividades correspondam, no presente caso, a uma das exceções previstas no RGPD (n.os 71 a 74 e disp.).

6. Requisitos de licitude de um tratamento de dados pessoais

[28] Artigo 4.°, n.° 7, do RGPD.
[29] Artigo 15.° do RGPD.

Acórdão de 16 de dezembro de 2008 (Grande Secção), Huber (C-524/06, EU:C:2008:724) [30]

O Serviço Federal das Migrações e Refugiados (Bundesamt für Migration und Flüchtlinge, Alemanha) assegurava a gestão de um registo central dos estrangeiros que reunia certos dados pessoais relativos aos estrangeiros que residiam no território alemão por um período superior a três meses. O registo era utilizado para fins estatísticos pelos serviços de segurança e de polícia, assim como pelas autoridades judiciárias, no exercício de competências no domínio do processo penal e em investigações de atos criminosos ou de atos que pusessem em perigo a ordem pública.

H. Huber, nacional austríaco, instalou-se na Alemanha em 1996 para aí exercer a profissão de agente de seguros por conta própria. Por se considerar discriminado devido ao tratamento de que eram objeto os seus dados constantes do registo em causa, uma vez que essa base de dados não existia para os nacionais alemães, H. Huber requereu a supressão desses dados.

Neste contexto, o Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Tribunal Administrativo Superior do Land da Renânia do Norte-Vestefália, Alemanha), chamado a conhecer do litígio, interrogou o Tribunal de Justiça sobre a compatibilidade com o direito da União do tratamento de dados pessoais realizado no registo em causa.

O Tribunal recordou, em primeiro lugar, que o direito de residência de um cidadão da União no território de um Estado-Membro, do qual não é nacional, não é incondicional, podendo ser sujeito a limitações. Por isso, a utilização de um registo com a finalidade de dar apoio às autoridades encarregues da aplicação da legislação sobre o direito de residência é, em princípio, legítima e, dada a sua natureza, compatível com a proibição de discriminação em razão da nacionalidade constante do artigo 12.°, primeiro parágrafo, CE (atual artigo 18.°, primeiro parágrafo, TFUE). Todavia, tal registo não pode conter informações diferentes das necessárias para essa finalidade na aceção da diretiva sobre a proteção de dados pessoais (n.os 54, 58, 59).

No que diz respeito ao conceito de «necessidade» do tratamento na aceção do artigo 7.°, alínea e), da Diretiva 95/46, o Tribunal começou por recordar que se tratava de um conceito autónomo do direito da União que deve receber uma interpretação suscetível de cumprir plenamente o objetivo da Diretiva 95/46, definido no seu artigo 1.°, n.° 1. Em seguida, o Tribunal constatou que um sistema de tratamento de dados pessoais só é conforme ao direito da União se contiver unicamente os dados necessários à aplicação dessa legislação pelas referidas autoridades e o seu caráter centralizado permitir uma aplicação mais eficaz dessa legislação no que respeita ao direito de residência dos cidadãos da União Europeia que não são nacionais desse Estado-Membro.

Em todo o caso, não se podem considerar necessários, na aceção do artigo 7.°, alínea e), da Diretiva 95/46, a conservação e o tratamento de dados pessoais nominativos no âmbito de um registo como o registo central dos estrangeiros para fins estatísticos (n.os 52, 66 e 68).

Por outro lado, no que respeita à questão da utilização das informações contidas no registo para efeitos de luta contra a criminalidade, o Tribunal observou, nomeadamente, que este

[30] Este acórdão foi apresentado no Relatório Anual de 2008, p. 45.

objetivo visa a repressão dos crimes e dos delitos cometidos, independentemente da nacionalidade dos seus autores. Por esta razão, para um Estado-Membro, a situação dos seus nacionais não pode ser diferente da dos cidadãos da União que não são nacionais desse Estado-Membro e residem no seu território, face ao objetivo de combate à criminalidade. Por conseguinte, a diferença de tratamento entre esses nacionais e esses cidadãos da União Europeia induzida pelo tratamento sistemático dos dados pessoais respeitantes unicamente aos cidadãos da União Europeia, que não são nacionais do Estado-Membro em causa, com o objetivo de combater a criminalidade, constitui uma discriminação proibida pelo artigo 12.°, primeiro parágrafo, CE (n.os 78 a 80).

Acórdão de 24 de novembro de 2011, ASNEF e FECEMD (C-468/10 e C-469/10, EU:C:2011:777)

A Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), por um lado, e a Federación de Comercio Eletrónico y Marketing Direto (FECEMD), por outro, interpuseram no Tribunal Supremo (Espanha) um recurso contencioso de anulação de vários artigos do Real Decreto 1720/2007 que aplicava a Lei Orgânica 15/1999, que tinha transposto a Diretiva 95/46.

Em especial, a ASNEF e a FECEMD consideravam que, para permitir o tratamento de dados pessoais na falta de consentimento da pessoa em causa, o direito espanhol acrescentava um requisito que não existe na Diretiva 95/46, exigindo que os referidos dados constem de «fontes acessíveis ao público», tal como enumeradas no artigo 3.°, alínea j), da Lei Orgânica 15/1999. A este respeito, alegaram que essa lei e o Real Decreto 1720/2007 restringiam o alcance do artigo 7.°, alínea f), da Diretiva 95/46, que sujeita o tratamento de dados de caráter pessoal, na falta do consentimento da pessoa em causa, a um requisito exclusivamente relativo ao interesse legítimo prosseguido pelo responsável pelo tratamento ou pelo terceiro ou terceiros a quem os dados sejam comunicados.

A este respeito, o Tribunal salientou, antes de mais, que o artigo 7.° da Diretiva 95/46 prevê uma lista exaustiva e taxativa dos casos em que um tratamento de dados pessoais pode ser considerado lícito na falta de consentimento da pessoa em causa. Por conseguinte, os Estados-Membros também não podem introduzir, ao abrigo do artigo 5.° da referida diretiva, outros princípios relativos à legitimação de tratamentos de dados pessoais além dos enunciados no artigo 7.° nem alterar, através de exigências suplementares, o alcance dos princípios previstos no referido artigo 7.° Com efeito, o artigo 5.° só autoriza os Estados-Membros a precisar, nos limites do capítulo II da referida diretiva e, logo, do artigo 7.° da mesma, as condições em que os tratamentos de dados pessoais são lícitos (n.os 30, 32 e 33).

Em particular, para efetuarem a necessária ponderação dos direitos e interesses opostos em causa, prevista no artigo 7.°, alínea f), da referida diretiva, os Estados-Membros podem prever princípios orientadores. Os Estados-Membros podem igualmente tomar em consideração o facto de a gravidade da violação dos direitos fundamentais da pessoa em causa no tratamento poder variar em função da questão de saber se os referidos dados em causa já constam, ou não, de fontes acessíveis ao público (n.os 44 e 46).

Contudo, o Tribunal considerou que já não está em causa uma especificação na aceção do artigo 5.° da Diretiva 95/46 se uma regulamentação nacional exclui a possibilidade de algumas categorias de dados pessoais serem tratadas, prescrevendo, para essas categorias, de forma

definitiva, o resultado da ponderação dos direitos e interesses opostos, sem autorizar um resultado diferente devido a circunstâncias particulares de um caso concreto. Por conseguinte, o Tribunal concluiu que o artigo 7.°, alínea f), da Diretiva 95/46 se opõe a que um Estado-Membro exclua de forma categórica e generalizada a possibilidade de algumas categorias de dados pessoais serem tratadas sem permitir que num caso específico se proceda a uma ponderação dos direitos e interesses opostos em causa (n.os 47 e 48).

Acórdão de 19 de outubro de 2016, Breyer (C-582/14, EU:C:2016:779)

Neste acórdão (v. igualmente a rubrica II.2., intitulada «Conceito de «dados pessoais») o Tribunal também se pronunciou sobre a questão de saber se o artigo 7.°, alínea f), da Diretiva 95/46 se opõe a uma disposição de direito nacional nos termos da qual o prestador de serviços de meios de comunicação em linha apenas pode recolher e utilizar dados pessoais de um utilizador sem o seu consentimento, na medida em que tal seja necessário para permitir e faturar a utilização concreta do meio de comunicação em linha por parte desse utilizador, e nos termos da qual a finalidade de garantir o funcionamento geral do meio de comunicação em linha não pode justificar a sua utilização após o termo da sessão de consulta em curso.

O Tribunal declarou que o artigo 7.°, alínea f), da Diretiva 95/46 se opõe à regulamentação em causa. Com efeito, ao abrigo desta disposição, o tratamento de dados pessoais, na aceção da mesma, é considerado lícito se o tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa. Ora, no caso em apreço, a regulamentação alemã excluía de forma categórica e generalizada a possibilidade de algumas categorias de dados pessoais serem tratadas, sem permitir uma ponderação dos direitos e interesses opostos em causa num caso específico. Ao fazê-lo, reduziu ilicitamente o âmbito deste princípio previsto no artigo 7.°, alínea f), da Diretiva 95/46, impedindo que o objetivo de garantir a capacidade geral de funcionamento dos sítios Internet do meio de comunicação em linha pudesse ser objeto de ponderação com o interesse ou os direitos e liberdades fundamentais dos utilizadores (n.os 62 a 64 e disp. 2).

Acórdão de 4 de maio de 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Este processo inscreve-se no âmbito de um litígio que opunha a polícia nacional letã à Rīgas satiksme, sociedade de tróleis da cidade de Riga, relativo a um pedido de comunicação dos dados de identificação do autor de um acidente. No caso em apreço, num acidente de circulação rodoviária, um taxista tinha estacionado o seu veículo junto ao passeio. No momento em que o trólei da Rīgas satiksme circulava junto a este táxi, o passageiro que ocupava o banco traseiro do referido táxi abriu a porta, que bateu na carroçaria do trólei, danificando-a. Para instaurar uma ação cível, a Rīgas satiksme pediu, nomeadamente, à polícia nacional a comunicação dos dados de identificação do autor do acidente. A polícia tinha recusado comunicar o número do documento de identificação e o endereço do passageiro bem como os documentos relativos às declarações prestadas pelas pessoas envolvidas no acidente pelo facto de os documentos relativos a um processo administrativo sancionatório só poderem ser comunicados às partes nesse processo, e de, no que respeita ao número de identificação e ao

endereço, a Lei de proteção dos dados das pessoas singulares proibir a divulgação de tais informações sobre particulares.

Nestas condições, o Augstākās tiesas Administratīvo lietu departaments (Supremo Tribunal, Secção de Contencioso Administrativo, Letónia) submeteu ao Tribunal a questão de saber se o artigo 7.°, alínea f), da Diretiva 95/46, impõe a obrigação de comunicar dados pessoais a um terceiro para permitir que este último instaure uma ação de indemnização num tribunal cível por um dano causado pela pessoa interessada na proteção desses dados e se o facto de essa pessoa ser menor pode ser relevante para a interpretação desta disposição.

O Tribunal declarou que o artigo 7.°, alínea f), da Diretiva 95/46 deve ser interpretado no sentido de que não impõe a obrigação de comunicar dados pessoais a um terceiro a fim de lhe permitir instaurar uma ação de indemnização num tribunal cível por um dano causado pela pessoa interessada na proteção desses dados. Todavia, a referida disposição não se opõe a essa comunicação no caso de a mesma ser efetuada com base no direito nacional, respeitando os requisitos previstos nesta disposição (n.os 27, 34 e disp.).

Neste contexto, o Tribunal observou que, sem prejuízo das verificações a efetuar a este respeito pelo juiz nacional, não se afigura justificado, em condições como as que estão em causa no processo principal, recusar a uma parte lesada a comunicação dos dados pessoais necessária à propositura de uma ação de indemnização contra o autor do dano ou, sendo caso disso, contra as pessoas que exerçam o poder parental, pelo facto de esse autor ser menor (n.° 33).

Acórdão de 27 de setembro de 2017, Puškár (C-73/16, EU:C:2017:725)

No processo principal, P. Puškár tinha interposto um recurso no Najvyšší súd Slovenskej republiky (Supremo Tribunal da República Eslovaca) requerendo que o Finančné riaditel'stvo (Direção de Finanças), todas as autoridades fiscais sob o seu controlo e o Kriminálny úrad finančnej správy (Serviço de Luta contra a Criminalidade Financeira) fossem intimados a não inscrever o seu nome na lista de pessoas consideradas pela Direção de Finanças como testas de ferro, elaborada no âmbito da cobrança de impostos, e cuja atualização era assegurada pela Direção de Finanças, bem como pelo departamento de luta contra a criminalidade financeira (a seguir «lista controvertida»). Além disso, tinha pedido que qualquer referência a seu respeito fosse suprimida dessas listas e do sistema informático da administração financeira.

Nestas condições, o Najvyšší súd Slovenskej republiky (Supremo Tribunal da República Eslovaca) submeteu ao Tribunal a questão de saber, nomeadamente, se o direito ao respeito da vida privada e familiar e das comunicações, consagrado no artigo 7.°, e o direito à proteção dos dados pessoais, consagrado no artigo 8.° da Carta, podem ser interpretados no sentido de que um Estado-Membro não pode, sem o consentimento do interessado, elaborar listas de dados pessoais para efeitos da cobrança de impostos, na medida em que a obtenção de dados pessoais pelas autoridades públicas para combater a fraude fiscal poderia, em si mesma, constituir um risco.

O Tribunal concluiu que o artigo 7.°, alínea e), da Diretiva 95/46 não se opõe a um tratamento de dados pessoais pelas autoridades de um Estado-Membro para efeitos da cobrança de impostos e de luta contra a fraude fiscal, como o que consistiu na criação da lista controvertida

no processo principal, sem o consentimento das pessoas em causa, desde que, por um lado, essas autoridades tenham sido investidas pela legislação nacional de missões de interesse público, na aceção desta disposição, de que a criação dessa lista e a inscrição do nome das pessoas em causa sejam efetivamente adequadas e necessárias para alcançar os objetivos prosseguidos e de que haja indícios suficientes para presumir que a inscrição das pessoas em causa na lista é justificada e, por outro, de que estejam cumpridos todos os requisitos de licitude deste tratamento de dados pessoais impostos pela Diretiva 95/46 (n.° 117 e disp. 3).

A este respeito, o Tribunal declarou que incumbe ao órgão jurisdicional de reenvio verificar se a criação da lista controvertida é necessária para a execução das missões de interesse público em causa no processo principal, atendendo, designadamente, à finalidade exata da criação da lista controvertida, aos efeitos jurídicos a que estão sujeitas as pessoas que nela figuram e ao caráter público ou não dessa lista. Além disso, à luz do princípio da proporcionalidade, cabe ao órgão jurisdicional nacional verificar se a criação da lista controvertida e a inscrição na mesma do nome das pessoas em causa são adequadas para alcançar os objetivos prosseguidos e se não existem outras medidas menos restritivas para alcançar os referidos objetivos (n.os 111, 112 e 113).

Além disso, o Tribunal constatou que o facto de uma pessoa estar inscrita na lista controvertida pode pôr em causa alguns dos seus direitos. Com efeito, a inscrição nessa lista pode prejudicar a sua reputação e afetar as suas relações com as autoridades fiscais. De igual modo, esta inscrição pode afetar a presunção de inocência dessa pessoa, consagrada no artigo 48.°, n.° 1, da Carta, bem como a liberdade de empresa, prevista no artigo 16.° da Carta, das pessoas coletivas associadas às pessoas singulares inscritas na lista controvertida. Por conseguinte, tal afetação só pode ser adequada se houver indícios suficientes para suspeitar que a pessoa em causa ocupa de forma fictícia um cargo de direção nas pessoas coletivas que lhe estão associadas e que, desse modo, prejudica a cobrança dos impostos e a luta contra a fraude fiscal (n.° 114).

Por outro lado, o Tribunal considerou que se existirem motivos para restringir, ao abrigo do artigo 13.° da Diretiva 95/46, certos direitos previstos nos artigos 6.° e 10.° a 12.° desta diretiva, como o direito à informação da pessoa em causa, essa restrição deve ser necessária à proteção de um interesse mencionado no n.° 1 do referido artigo 13.°, como, designadamente, um interesse económico ou financeiro importante no domínio fiscal, e basear-se em medidas legislativas (n.° 116).

Acórdão de 11 de novembro de 2020, Orange Romania (C-61/19, EU:C:2020:901)

A Orange România fornece serviços de telecomunicações móveis no mercado romeno. Em 28 de março de 2018, a Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Autoridade Nacional de Supervisão do Tratamento dos Dados Pessoais, Roménia) aplicou-lhe uma coima por ter recolhido e conservado as cópias dos títulos de identidade dos seus clientes sem o consentimento expresso destes últimos.

Segundo a ANSPDCP, no período compreendido entre 1 e 26 de março de 2018, a Orange România celebrou contratos de fornecimento de serviços de telecomunicação móvel que contêm uma cláusula segundo a qual os clientes foram informados e deram o seu

consentimento para a recolha e a conservação de uma cópia do seu título de identidade para fins de identificação. A opção relativa a essa cláusula foi validada pelo responsável pelo tratamento antes da assinatura do contrato.

Foi neste contexto que o Tribunalul București (Tribunal Regional de Bucareste, Roménia) pediu ao Tribunal de Justiça que precisasse as condições nas quais o consentimento dos clientes no tratamento de dados pessoas pode ser considerado válido.

O Tribunal recorda, antes de mais, que o direito da União [31] prevê uma lista dos casos em que um tratamento de dados pessoais pode ser considerado lícito. Em especial, o consentimento da pessoa em causa deve ser livre, específico, informado e inequívoco [32]. A este respeito, o consentimento não é validamente dado em caso de silêncio, de opções validadas por defeito ou em caso de inatividade (n.os 34, 36, 37 e 39).

Além disso, quando o consentimento da pessoa em causa for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, essa declaração deve ser apresentada de modo inteligível e de fácil acesso e numa linguagem clara e simples. Para assegurar à pessoa em causa uma verdadeira liberdade de escolha, as estipulações contratuais não devem induzi-la em erro quanto à possibilidade de celebrar o contrato mesmo que se recuse a dar o seu consentimento para o tratamento dos seus dados (n.os 34, 36, 37, 39 e 41).

O Tribunal precisa que, sendo a Orange România a responsável pelo tratamento dos dados pessoais, deve poder demonstrar a licitude do tratamento desses dados e, portanto, no caso concreto, a existência de um consentimento válido dos seus clientes. A este respeito, uma vez que não se afigura que os clientes em causa tenham validado eles próprios a opção relativa à recolha e à conservação das cópias do seu título de identidade, o simples facto de essa opção ter sido validada não é suscetível de demonstrar uma manifestação positiva do seu consentimento. Cabe ao órgão jurisdicional de reenvio proceder às necessárias verificações para esse fim (n.os 42 e 46).

Cabe igualmente ao órgão jurisdicional, segundo o Tribunal, avaliar se as estipulações contratuais em causa eram ou não suscetíveis de induzir os clientes em causa em erro quanto à possibilidade de celebrar o contrato não obstante a recusa de autorizar o tratamento dos seus dados, na falta de indicações sobre essa possibilidade. Além disso, em caso de recusa de um cliente de autorizar o tratamento dos seus dados, o Tribunal observa que a Orange România exigia que este declarasse por escrito que não autorizava a recolha nem a conservação da cópia do seu título de identidade. Segundo o Tribunal, tal exigência suplementar é suscetível de afetar indevidamente a livre escolha de se opor a essa recolha e a essa conservação. De qualquer modo, uma vez que essa sociedade deve demonstrar que os seus clientes manifestaram, através de um comportamento ativo, o seu consentimento para o tratamento dos seus dados pessoais, esta sociedade não lhes pode exigir que manifestem a sua recusa ativamente (n.os 49 a 51).

O Tribunal conclui, portanto, que um contrato relativo ao fornecimento de serviços de telecomunicações que contém uma cláusula segundo a qual a pessoa em causa foi informada e

[31] Artigo 7.°, da Diretiva 95/46 e artigo 6.°, do RGPD.

[32] Artigo 2.°, alínea h), da Diretiva 95/46 e artigo 4, ponto 11, do RGPD.

deu o seu consentimento para a recolha bem como para a conservação de uma cópia do seu título de identidade para fins de identificação não é suscetível de demonstrar que essa pessoa deu validamente o seu consentimento para essa recolha e para essa conservação, quando a opção relativa a essa cláusula foi validada pelo responsável pelo tratamento dos dados antes da assinatura desse contrato, quando as estipulações contratuais do referido contrato são suscetíveis de induzir a pessoa em causa em erro quanto à possibilidade de celebrar o contrato em questão mesmo que se recuse a autorizar o tratamento dos seus dados, ou quando a livre escolha de se opor a essa recolha e a essa conservação é afetada indevidamente por esse responsável, ao exigir que a pessoa em causa, a fim de se recusar a dar o seu consentimento, preencha um formulário suplementar onde fique registada essa recusa (n.° 52 e disp.).

Acórdão de 12 de maio de 2021 (Grande Secção), Bundesrepublik Deutschland (Alerta vermelho da Interpol) (C-505/19, EU:C:2021:376)

Em 2012, a Organização Internacional de Polícia Criminal (a seguir «Interpol»), a pedido dos Estados Unidos e com base num mandado de detenção emitido pelas autoridades desse país, publicou um alerta vermelho relativo a WS, cidadão alemão, com vista à sua eventual extradição. Quando uma pessoa contra quem foi emitido esse alerta é localizada num Estado-Membro da Interpol, este último deve, em princípio, proceder à sua detenção provisória ou controlar ou restringir as suas deslocações.

Todavia, na Alemanha, antes da publicação desse alerta vermelho, tinha sido instaurado contra WS um processo de inquérito que segundo o órgão jurisdicional de reenvio era relativo aos mesmos factos que tinham estado na origem do referido alerta. Esse processo foi definitivamente arquivado em 2010, após o pagamento de uma quantia pecuniária por WS, em conformidade com um procedimento específico de acordo previsto no direito penal alemão. Posteriormente, o Bundeskriminalamt (Serviço Federal de Polícia Judiciária, Alemanha) informou a Interpol de que considerava que, em razão desse anterior processo, o princípio *ne bis in idem* era aplicável no caso em apreço. Este princípio, consagrado tanto no artigo 54.° da Convenção de aplicação do Acordo de Schengen [33] como no artigo 50.° da Carta, proíbe, nomeadamente, que possa ser instaurado novo processo pelo mesmo ilícito contra uma pessoa que já tenha sido julgada por decisão definitiva.

Em 2017, WS propôs uma ação contra a Alemanha no Verwaltungsgericht Wiesbaden (Tribunal Administrativo de Wiesbaden, Alemanha) para que fosse ordenado a esse Estado-Membro que tomasse as medidas necessárias à retirada desse alerta vermelho. A este respeito, além de uma violação do princípio *ne bis in idem*, WS invoca uma violação do seu direito à livre circulação, garantido pelo artigo 21.° TFUE, por não se poder deslocar a um Estado parte no Acordo de Schengen, ou a um Estado-Membro, sem correr o risco de ser detido. Considera igualmente que, por causa dessas violações, o tratamento dos seus dados pessoais, que figuram no alerta

[33] Convenção de aplicação do Acordo de Schengen, de 14 de junho de 1985, entre os Governos dos Estados da União Económica Benelux, da República Federal da Alemanha e da República Francesa relativo à supressão gradual dos controlos nas fronteiras comuns, assinada em Schengen (Luxemburgo) em 19 de junho de 1990 e entrada em vigor em 26 de março de 1995 (JO 2000, L 239, p. 19, a seguir «CAAS»).

vermelho, é contrário à Diretiva 2016/680, relativa à proteção dos dados pessoais em matéria penal [34].

Foi neste contexto que o Verwaltungsgericht Wiesbaden decidiu interrogar o Tribunal de Justiça sobre a aplicação do princípio *ne bis in idem*, mais precisamente sobre a possibilidade de proceder à detenção provisória de uma pessoa contra quem foi emitido um alerta vermelho numa situação como a que está em causa. Além disso, caso este princípio seja aplicável, esse órgão jurisdicional pretende saber quais as consequências para o tratamento, pelos Estados-Membros, dos dados pessoais contidos no referido alerta.

No seu acórdão de Grande Secção, o Tribunal declara, nomeadamente, que as disposições da Diretiva 2016/680, lidas à luz do artigo 54.° da CAAS e do artigo 50.° da Carta, devem ser interpretadas no sentido de que não se opõem ao tratamento de dados pessoais que figurem num alerta vermelho emitido pela Interpol, enquanto não for demonstrado, através dessa decisão judicial, que o princípio *ne bis in idem* é aplicável aos factos em que esse alerta se baseia, desde que o referido tratamento cumpra os requisitos previstos nessa diretiva (n.° 121 e disp. 2).

No que diz respeito à questão relativa aos dados pessoais que figuram num alerta vermelho da Interpol, o Tribunal indica que qualquer operação aplicada a esses dados, como o respetivo registo nas listas de pessoas procuradas de um Estado-Membro, constitui um «tratamento» abrangido pela Diretiva 2016/680 [35]. Além disso, considera, por um lado, que esse tratamento prossegue uma finalidade legítima e, por outro, que o mesmo não pode ser considerado ilícito apenas pelo facto de o princípio *ne bis in idem* poder ser aplicável aos factos em que se baseia o alerta vermelho [36]. De resto, o tratamento em causa por parte das autoridades dos Estados-Membros pode revelar-se indispensável, precisamente para verificar se o referido princípio é aplicável (n.os 111, 114, 116, 117 e 119).

Nestas condições, o Tribunal declara igualmente que a Diretiva 2016/680, lida à luz do artigo 54.° da CAAS e do artigo 50.° da Carta, não se opõe ao tratamento de dados pessoais que figuram num alerta vermelho enquanto uma decisão judicial definitiva não tiver demonstrado que o princípio *ne bis in idem* é aplicável ao caso em apreço. Todavia, tal tratamento deve respeitar os requisitos previstos por esta diretiva. Nesta perspetiva, o tratamento em causa deve ser necessário, nomeadamente, para o exercício de uma atribuição por parte de uma autoridade nacional competente, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais [37] (n.° 121 e disp. 2).

Em contrapartida, quando for aplicável o princípio *ne bis in idem*, o registo, nas listas de pessoas procuradas dos Estados-Membros, dos dados pessoais que figuram num alerta vermelho da Interpol já não é necessário, uma vez que já não podem ser instaurados processos penais contra a pessoa em causa pelos factos abrangidos pelo referido alerta e, por conseguinte, a

[34] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO 2016, L 119, p. 89).

[35] V. artigos 2.°, n.° 1, e 3.°, ponto 2, da Diretiva 2016/680.

[36] V. artigos 4.°, n.° 1, alínea b), e 8.°, n.° 1, da Diretiva 2016/680.

[37] V. artigos 1.°, n.° 1, e 8.°, n.° 1, da Diretiva 2016/680.

mesma já não pode ser detida por esses mesmos factos. Daqui resulta que deve ser dada à pessoa em causa a possibilidade de pedir o apagamento dos seus dados. Se, todavia, esse registo for mantido, deve ser acompanhado da indicação de que a pessoa em causa já não pode ser julgada num Estado-Membro ou num Estado contratante pelos mesmos factos, em razão do princípio *ne bis in idem* (n.º 120).

Acórdão de 22 de junho de 2021 (Grande Secção), Latvijas Republikas Saeima (Pontos de penalização) (C-439/19, EU:C:2021:504)

Neste acórdão (v. igualmente rubrica II.3., intitulada « Conceito de "tratamento de dados pessoais»), o Tribunal declara que o RGPD se opõe à legislação que obriga a Ceļu satiksmes drošības direkcija CSDD (Direção da Segurança Rodoviária, Letónia) (a seguir «CSDD») a tornar acessíveis ao público os dados relativos aos pontos de penalização aplicados aos condutores de veículos por infrações rodoviárias, sem que a pessoa que pede o acesso tenha de demonstrar um interesse específico em obtê-los. O Tribunal declarou que não está demonstrada a necessidade, nomeadamente à luz do objetivo de melhoria da segurança rodoviária invocado pelo governo letão, da comunicação dos dados pessoais relativos aos pontos de penalização aplicados por infrações rodoviárias. Além disso, segundo o Tribunal, nem o direito do público de aceder aos documentos oficiais nem o direito à liberdade de informação justificam tal legislação (n.os 113, 120 a 122 e disp. 2).

Neste contexto, o Tribunal sublinha que a melhoria da segurança rodoviária, pretendida pela legislação letã, constitui um objetivo de interesse geral reconhecido pela União e que, por conseguinte, os Estados-Membros podem qualificar a segurança rodoviária como um «exercício de funções de interesse público» [38]. No entanto, não está demonstrada a necessidade do regime letão de comunicação dos dados pessoais relativos aos pontos de penalização para assegurar o objetivo visado. Com efeito, por um lado, o legislador letão dispõe de uma multiplicidade de vias de atuação que lhe teriam permitido alcançar esse objetivo por outros meios menos atentatórios dos direitos fundamentais das pessoas em causa. Por outro lado, importa ter em conta o caráter sensível dos dados relativos aos pontos de penalização e o facto de a sua comunicação ao público ser suscetível de constituir uma ingerência grave nos direitos ao respeito pela vida privada e à proteção dos dados pessoais, uma vez que a mesma pode suscitar a desaprovação social e a estigmatização da pessoa em causa (n.os 109 a 113).

Além disso, o Tribunal considera que, tendo em conta o caráter sensível destes dados e a gravidade dessa ingerência nestes dois direitos fundamentais, estes direitos prevalecem tanto sobre o interesse do público em aceder a documentos oficiais, como o registo nacional de veículos e condutores, como sobre o direito à liberdade de informação (n.os 120 e 121).

Por outro lado, por razões idênticas, o Tribunal declara que o RGPD se opõe igualmente à legislação letã na medida em que autoriza a CSDD a comunicar os dados relativos aos pontos de penalização aplicados aos condutores de veículos por infrações rodoviárias a operadores económicos para que estes últimos os possam reutilizar e comunicar ao público (n.º 126 e disp. 3).

[38] Nos termos do artigo 6.º, n.º 1, alínea e), do RGPD, o tratamento de dados pessoais é lícito se for «necessário ao exercício de funções de interesse público [...]».

Por último, o Tribunal declara que o princípio do primado do direito da União se opõe a que o órgão jurisdicional de reenvio, chamado a pronunciar-se num recurso contra a legislação letã, qualificada pelo Tribunal de incompatível com o direito da União, decida manter os efeitos jurídicos dessa legislação até à data da prolação do acórdão que decide definitivamente esse recurso (n.° 137 e disp. 4).

III. Tratamento de dados pessoais na aceção da Diretiva 2002/58/CE

Acórdão de 2 de outubro de 2018 (Grande Secção), Ministerio Fiscal (C-207/16, EU:C:2018:788) [39]

Neste processo estava em causa o indeferimento, por um juiz de instrução espanhol, de um pedido apresentado no quadro da investigação de um roubo de uma carteira e de um telemóvel. Em particular, a polícia judiciária tinha pedido autorização ao referido juiz para aceder aos dados de identificação dos utilizadores dos números de telefone que tinham sido ativados a partir do telefone roubado, durante um período de doze dias a contar da data do roubo. O indeferimento assentou na circunstância de os factos que estavam na origem do inquérito penal não serem constitutivos de uma infração «grave» – ou seja, de acordo com o direito espanhol, uma infração sancionada com uma pena de prisão superior a cinco anos – e que o acesso aos dados de identificação só era possível para este tipo de infração.

Depois de recordar que o acesso de autoridades públicas a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas, no quadro de um processo de instrução penal, é abrangido pelo âmbito de aplicação da Diretiva 2002/58, o Tribunal declarou que o acesso a dados, com vista à identificação dos titulares de cartões SIM ativados com um telemóvel roubado, como os apelidos, nomes próprios e, sendo caso disso, os endereços desses titulares, constitui uma ingerência nos direitos fundamentais ao respeito da vida privada e à proteção dos dados, consagrados pela Carta, mesmo que não se verifiquem circunstâncias que permitam qualificar esta ingerência de «grave» e sem que seja relevante que as informações relativas à vida privada em causa tenham ou não caráter sensível ou que os interessados tenham ou não sofrido eventuais inconvenientes devido a essa ingerência. Todavia, o Tribunal sublinhou que esta ingerência não apresenta uma gravidade tal que esse acesso deva ser limitado, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, à luta contra a criminalidade grave. Com efeito, embora a Diretiva 2002/58 enumere de forma exaustiva os objetivos que podem justificar a existência de uma regulamentação nacional que regule o acesso das autoridades públicas aos dados em causa e que, desse modo, derrogue o princípio da confidencialidade das comunicações eletrónicas, devendo este acesso dar efetiva e estritamente resposta a um desses objetivos, o Tribunal de Justiça observa que, no que respeita ao objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais, a redação da Diretiva 2002/58 não limita esse objetivo à luta contra as infrações graves, mas visa as «infrações penais» em geral (n.os 38, 42, 59 a 63 e disp.).

[39] Este acórdão foi apresentado no Relatório Anual de 2018, pp. 88 e 89.

Neste contexto, o Tribunal precisou que, embora, no seu Acórdão Tele2 Sverige e Watson e o. [40], tivesse declarado que apenas a luta contra a criminalidade grave pode justificar que as autoridades públicas acedam a dados pessoais que são conservados pelos fornecedores de serviços de comunicações, e que, tomados no seu conjunto, permitem tirar conclusões precisas a respeito da vida privada das pessoas cujos dados estão em causa, essa interpretação assentava no facto de o objetivo prosseguido por uma regulamentação que regula esse acesso ter de estar relacionada com a gravidade da ingerência nos direitos fundamentais em causa que tal operação implica. Assim, em conformidade com o princípio da proporcionalidade, uma ingerência grave só pode ser justificada por um objetivo de luta contra a criminalidade que deva igualmente ser qualificada de «grave». Em contrapartida, quando a ingerência não é grave, o referido acesso pode ser justificado por um objetivo de prevenção, de investigação, de deteção e de repressão de «infrações penais» em geral (n.os 54 a 57).

Neste caso concreto, o Tribunal considerou que o acesso limitado aos dados visados pelo pedido não podia ser qualificado de ingerência «grave» nos direitos fundamentais das pessoas cujos dados estavam em causa, uma vez que esses dados não permitiam tirar conclusões precisas a respeito da vida privada dessas pessoas. O Tribunal concluiu que a ingerência que um acesso a esses dados implica é, portanto, suscetível de ser justificada pelo objetivo de prevenção, de pesquisa, de deteção e de repressão de «infrações penais» em geral, sem que seja necessário que essas infrações sejam qualificadas de « graves » (n.os 61 e 62).

Acórdãos de 6 de outubro de 2020 (Grande Secção), Privacy International (C-623/17, EU:C:2020:790) e La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791) [41]

A jurisprudência relativa à conservação e ao acesso aos dados pessoais no domínio das comunicações eletrónicas, em particular o Acórdão Tele2 Sverige e Watson e o., em que o Tribunal considerou nomeadamente que os Estados-Membros não podiam impor aos prestadores de serviços de comunicações eletrónicas uma obrigação de conservação generalizada e indiferenciada de dados de tráfego e de localização, suscitou preocupações nalguns Estados, que receavam ter sido privados de um instrumento que consideram necessário à salvaguarda da segurança nacional e à luta contra a criminalidade.

Foi sobre este pano de fundo que foram submetidos ao Investigatory Powers Tribunal (Tribunal de Instrução, Reino Unido) (Privacy International, C-623/17), ao Conseil d'État (Conselho de Estado, em formação jurisdicional, França) (La Quadrature du Net e o., processo apensos C-511/18 e C-512/18) e à Cour constitutionnelle (Tribunal Constitucional, Bélgica) (Ordre des barreaux francophones et germanophone e o., C-520/18) litígios relativos à legalidade das regulamentações adotadas por alguns Estados-Membros nestes domínios, que preveem, em especial, uma obrigação de os prestadores de serviços de comunicações eletrónicas transmitirem a uma autoridade pública ou de conservarem de forma generalizada ou indiferenciada os dados dos utilizadores relativos ao tráfego e à localização.

Através de dois Acórdãos proferidos em Grande Secção, em 6 de outubro de 2020, o Tribunal de Justiça declarou, antes de mais, que a Diretiva 2002/58 se aplica a regulamentações nacionais que impõem aos fornecedores de serviços de comunicações eletrónicas que

[40] Acórdão do Tribunal de 21 de dezembro de 2016, *Tele2 Sverige e Watson e* o. (C-203/15 e C-698/15, EU:C:2016:970).
[41] Estes acórdãos foram apresentados no Relatório Anual de 2020, pp. 29 a 32

procedam, para efeitos de salvaguarda da segurança nacional e de luta contra a criminalidade, a tratamentos de dados pessoais, como a sua transmissão a autoridades públicas ou a sua conservação (n.º 49 e disp. 1 do Acórdão Privacy International e n.º 104 do Acórdão La Quadrature du Net e o.).

Em seguida, o Tribunal de Justiça recorda que a Diretiva 2002/58 [42] não permite que a derrogação da obrigação de princípio de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados e da proibição de armazenar esses dados se torne a regra. Isto implica que essa diretiva só autoriza os Estados-Membros a adotarem, nomeadamente para fins de segurança nacional, medidas legislativas destinadas a limitar o alcance dos direitos e das obrigações previstos por esta diretiva, nomeadamente a obrigação de garantir a confidencialidade das comunicações e dos dados de tráfego [43], no respeito dos princípios gerais do direito da União, entre os quais figura o princípio da proporcionalidade, e dos direitos fundamentais garantidos pela Carta [44] (n.os 59 e 60 do Acórdão Privacy International e n.os 111 e 113 do Acórdão La Quadrature du Net e o.).

Neste contexto, o Tribunal de Justiça considera, por um lado, no processo Privacy International, que a diretiva privacidade e comunicações eletrónicas, lida à luz da Carta, se opõe a uma regulamentação nacional que impõe aos fornecedores de serviços de comunicações eletrónicas, com vista à salvaguarda da segurança nacional, a transmissão generalizada e indiferenciada aos serviços de segurança e de informação dos dados de tráfego e de localização. Por outro lado, nos processos apensos La Quadrature du Net e o. e no processo Ordre des barreaux francophones et germanophone e o., o Tribunal de Justiça considera que esta mesma diretiva se opõe a medidas legislativas que imponham aos prestadores de serviços de comunicações eletrónicas, a título preventivo, uma conservação generalizada e indiferenciada dos dados de tráfego e de localização.

Com efeito, essas obrigações de transmissão e de conservação generalizada e indiferenciada de tais dados constituem ingerências particularmente graves nos direitos fundamentais garantidos pela Carta, sem que o comportamento das pessoas cujos dados estão em causa esteja relacionado com o objetivo prosseguido pela regulamentação em causa. De forma análoga, o Tribunal de Justiça interpreta o artigo 23.º, n.º 1, do RGPD, lido à luz da Carta, no sentido de que se opõe a uma regulamentação nacional que impõe aos prestadores de acesso a serviços de comunicação ao público em linha e aos prestadores de serviços de armazenamento a conservação generalizada e indiferenciada, nomeadamente, dos dados pessoais relativos a esses serviços (n.os 71, 82 e disp. 2 do Acórdão Privacy International e n.os 146, 168, 174, 177, 212, disp. 1 e 3 do Acórdão La Quadrature du Net e o.).

Em contrapartida, o Tribunal de Justiça considera que, em situações em que o Estado-Membro em causa se confronte com uma ameaça grave para a segurança nacional que revele ser real e atual ou previsível, a Diretiva 2002/58, lida à luz da Carta, não se opõe a que seja ordenado aos fornecedores de serviços de comunicações eletrónicas que conservem de forma generalizada e

42 Artigo 15.º, n.os 1 e 3, da Diretiva 2002/58.

43 Artigo 5.º, n.º 1, da Diretiva 2002/58.

44 Em especial, os artigos 7.º, 8.º e 11.º, bem como o artigo 52.º, n.º 1, da Carta.

indiferenciada dados de tráfego e de localização. Neste contexto, o Tribunal de Justiça precisa que a decisão que prevê essa injunção, por um período temporalmente limitado ao estritamente necessário, deve ser objeto de fiscalização efetiva, quer por um órgão jurisdicional quer por uma entidade administrativa independente, cuja decisão tenha efeito vinculativo, a fim de verificar a existência de uma dessas situações e o respeito das condições e das garantias previstas. Nestas mesmas condições, a referida diretiva também não se opõe à análise automatizada dos dados, nomeadamente os relativos ao tráfego e à localização de todos os utilizadores de meios de comunicações eletrónicas (n.os 137 a 139, 177 a 179, disp. 1 e 2 do Acórdão La Quadrature du Net e o.).

O Tribunal de Justiça acrescenta que a Diretiva 2002/58, lida à luz da Carta, não se opõe a medidas legislativas que permitam o recurso a uma conservação seletiva, temporalmente limitada ao estritamente necessário, dos dados de tráfego e de localização, que seja delimitada, com base em elementos objetivos e não discriminatórios, em função de categorias de pessoas em causa ou através de um critério geográfico. Do mesmo modo, essa diretiva não se opõe a medidas desse tipo que prevejam uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma comunicação, desde que o período de conservação se limite ao estritamente necessário, nem a medidas que prevejam essa conservação dos dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicas, não estando os Estados-Membros, neste último caso, obrigados a limitar temporalmente a conservação. Além disso, a referida diretiva não se opõe a uma medida legislativa que permita o recurso a uma conservação rápida dos dados de que dispõem os prestadores de serviços quando se verifiquem situações em que seja necessário conservá-los, além dos prazos legais de conservação de dados, para efeitos de elucidação de infrações penais graves ou de ofensas à segurança nacional, quando essas infrações ou violações já tenham sido constatadas ou quando se possa razoavelmente suspeitar da sua existência (n.os 161, 163, 168 e disp. 1 do Acórdão La Quadrature du Net e o.).

Além disso, o Tribunal de Justiça considera que a Diretiva 2002/58, lida à luz da Carta, não se opõe a uma regulamentação nacional que impõe aos fornecedores de serviços de comunicações eletrónicas que recorram à recolha em tempo real, nomeadamente, de dados de tráfego e de localização, quando essa recolha se limite às pessoas relativamente às quais existe uma razão válida para suspeitar que estão envolvidas, de uma maneira ou de outra, em atividades terroristas e quando a mesma esteja sujeita a fiscalização prévia, efetuada por um tribunal ou por uma entidade administrativa independente, cuja decisão tenha efeito vinculativo, garantindo que essa recolha em tempo real só é autorizada no limite do estritamente necessário. Em caso de urgência, a fiscalização deve ocorrer no mais curto espaço de tempo (n.° 192 e disp. 2 do Acórdão La Quadrature du Net e o.).

Por último, o Tribunal de Justiça aborda a questão da manutenção dos efeitos no tempo de uma regulamentação nacional considerada incompatível com o direito da União. A este respeito, considera que um órgão jurisdicional nacional não pode aplicar uma disposição do seu direito nacional que o habilita a limitar no tempo os efeitos de uma declaração de ilegalidade que lhe incumbe, relativamente a uma regulamentação nacional que impõe aos fornecedores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e de localização, considerada incompatível com a Diretiva 2002/58, lida à luz da Carta.

Dito isto, para dar uma resposta útil ao órgão jurisdicional nacional, o Tribunal de Justiça lembra que a admissibilidade e a apreciação das provas obtidas através de uma conservação de dados contrária ao direito da União, no âmbito de um processo penal instaurado contra pessoas suspeitas de atos de criminalidade grave, pertence, no estado atual do direito da União, unicamente ao direito nacional. Todavia, o Tribunal de Justiça precisa que a Diretiva 2002/58, interpretada à luz do princípio da efetividade, exige que o tribunal criminal nacional afaste as provas obtidas através de uma conservação generalizada e indiferenciada dos dados de tráfego e de localização incompatível com o direito da União, no âmbito desse processo penal, se as pessoas suspeitas de atos de criminalidade não puderem tomar eficazmente posição sobre essas provas (n.os 222, 228 e disp. 4 do Acórdão La Quadrature du Net e o.)

Acórdão de 2 de março de 2021 (Grande Secção), Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152)

Na Estónia, foi instaurado um processo penal contra H. K. por furto, por utilização do cartão bancário de um terceiro e por violência contra pessoas que participam num processo judicial. Pela prática destes crimes, H. K. foi condenada em primeira instância numa pena privativa de liberdade de dois anos. Esta decisão foi posteriormente confirmada em sede de recurso. Os relatórios em que assenta a condenação por esses crimes foram elaborados, designadamente, com base em dados pessoais gerados no âmbito do fornecimento de serviços de comunicação eletrónicos. O Riigikohus (Supremo Tribunal, Estónia), para o qual H. K. interpôs recurso de cassação, manifestou dúvidas quanto à compatibilidade com o direito da União [45] das condições em que os serviços de inquérito tiveram acesso a esses dados.

Essas dúvidas dizem respeito, em primeiro lugar, à questão de saber se a duração do período durante o qual os serviços de inquérito tiveram acesso aos dados constitui um critério que permita apreciar a gravidade da ingerência, a que esse acesso corresponde, nos direitos fundamentais da pessoa em questão. Assim, o órgão jurisdicional de reenvio tem dúvidas quanto à questão de saber se o objetivo de luta contra a criminalidade em geral, e não apenas de luta contra a criminalidade grave, é suscetível de justificar tal ingerência nos casos em que o referido período é muito curto ou em que a quantidade dos dados recolhidos é muito limitada. Em segundo lugar, o órgão jurisdicional de reenvio teve dúvidas quanto à possibilidade de considerar o Ministério Público estónio, tendo em conta as diferentes missões que lhe são confiadas pela regulamentação nacional, uma autoridade administrativa «independente» na aceção do Acórdão Tele2 Sverige e Watson e o. [46], suscetível de autorizar o acesso da autoridade encarregada do inquérito aos dados em questão.

Com o seu acórdão, proferido em Grande Secção, o Tribunal de Justiça declara que a Diretiva 2002/58, lida à luz da Carta, se opõe a uma regulamentação nacional que permite o acesso das autoridades públicas a dados relativos ao tráfego ou a dados de localização, suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados e

[45] Mais precisamente, com o 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.

[46] Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, n.° 120.

de permitir tirar conclusões precisas sobre a sua vida privada, para fins de prevenção, de investigação, de deteção e de repressão de infrações penais, sem que esse acesso esteja circunscrito a processos que visem a luta contra a criminalidade grave ou a prevenção de ameaças graves à segurança pública. Segundo o Tribunal, a duração do período em relação ao qual o acesso aos referidos dados é solicitado e a quantidade ou a natureza dos dados disponíveis em relação a esse período não tem incidência a este respeito. Além disso, o Tribunal considera que esta mesma diretiva, lida à luz da Carta, se opõe a uma regulamentação nacional que atribui competência ao Ministério Público para autorizar o acesso de uma autoridade pública aos dados relativos ao tráfego e aos dados de localização a fim de conduzir uma instrução penal (n.os 45, 59, disp. 1 e 2).

No que respeita ao objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais, prosseguido pela regulamentação em causa, em conformidade com o princípio da proporcionalidade, o Tribunal considera que só os objetivos de luta contra a criminalidade grave ou de prevenção de ameaças graves para a segurança pública podem justificar o acesso das autoridades públicas a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de permitir tirar conclusões precisas sobre a vida privada das pessoas em questão sem que outros fatores relativos à proporcionalidade de um pedido de acesso, como a duração do período em relação ao qual o acesso a esses dados é solicitado, possam ter por efeito que o objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral seja suscetível de justificar esse acesso (n.os 33 e 35).

Quanto à competência atribuída ao Ministério Público para autorizar o acesso de uma autoridade pública aos dados relativos ao tráfego e aos dados de localização a fim de dirigir uma instrução penal, o Tribunal recorda que cabe ao direito nacional determinar as condições em que os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes o acesso aos dados de que dispõem. No entanto, para cumprir a exigência de proporcionalidade, tal regulamentação deve prever regras claras e precisas que regulem o alcance e a aplicação da medida em causa e que imponham exigências mínimas, de modo que as pessoas cujos dados pessoais foram conservados disponham de garantias suficientes que permitam proteger eficazmente esses dados contra os riscos de abuso. Essa regulamentação deve ser legalmente vinculativa em direito interno e indicar em que circunstâncias e sob que condições uma medida que preveja o tratamento desses dados pode ser tomada, garantindo, assim, que a ingerência seja limitada ao estritamente necessário (n.° 48).

Segundo o Tribunal, a fim de garantir, na prática, o pleno respeito destes requisitos, é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja, em princípio, sujeito a uma fiscalização prévia, efetuada por um órgão jurisdicional ou por uma entidade administrativa independente e que a decisão desse órgão jurisdicional ou dessa entidade seja tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de repressão de infrações penais. Em caso de urgência devidamente justificada, a fiscalização deve ser efetuada dentro de prazos curtos (n.° 51).

A este respeito, o Tribunal precisa que a fiscalização prévia exige, designadamente, que o órgão jurisdicional ou a entidade encarregada de efetuar essa fiscalização disponha de todas as atribuições e apresente todas as garantias necessárias com vista a assegurar uma conciliação

dos diferentes interesses e direitos em causa. No que respeita mais especificamente a um inquérito penal, tal fiscalização exige que esse órgão jurisdicional ou essa entidade possa assegurar um justo equilíbrio entre, por um lado, os interesses ligados às necessidades do inquérito no âmbito da luta contra a criminalidade e, por outro, os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas às quais o acesso diz respeito. Quando essa fiscalização não é efetuada por um órgão jurisdicional mas por uma entidade administrativa independente, esta deve gozar de um estatuto que lhe permita agir, quando exerce as suas missões, de maneira objetiva e imparcial sendo que, para esse efeito, a mesma deve estar ao abrigo de qualquer influência externa (n.os 52 e 53).

Segundo o Tribunal, daqui resulta que a exigência de independência, a que está sujeita a autoridade encarregada de exercer a fiscalização prévia, impõe que essa autoridade tenha a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, de modo a que a primeira esteja em condições de exercer essa fiscalização de maneira objetiva e imparcial ao abrigo de qualquer influência externa. Em especial, no domínio penal, a exigência de independência implica que a autoridade encarregada dessa fiscalização prévia, por um lado, não esteja envolvida na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal. Ora, não é esse o caso de um Ministério Público que dirige o inquérito e, sendo caso disso, deduz acusação. Daqui resulta que o Ministério Público não está em condições de efetuar a fiscalização prévia acima referida (n.os 54, 55 e 57).

IV. Transferência dos dados pessoais para países terceiros

Acórdão de 6 de novembro de 2003 (Assembleia Plenária), Lindqvist (C-101/01, EU:C:2003:596) [47]

Neste processo (v. igualmente rubrica II.3., intitulada «Conceito de 'tratamento de dados pessoais'»), o órgão jurisdicional de reenvio pretendia, em particular, saber se B. Lindqvist tinha procedido a uma transferência de dados para um país terceiro na aceção da diretiva.

O Tribunal de Justiça declarou que não existe uma «transferência para um país terceiro de dados pessoais» na aceção do artigo 25.° da Diretiva 95/46, quando uma pessoa que se encontra num Estado-Membro insere dados pessoais numa página Internet de uma pessoa singular ou coletiva que alberga o sítio Internet no qual a página pode ser consultada, e que está estabelecida nesse mesmo Estado ou noutro Estado-Membro, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros (n.° 71 e disp. 4).

Com efeito, atendendo, por um lado, ao estado de evolução da Internet à época da elaboração da Diretiva 95/46 e, por outro, à ausência de critérios aplicáveis à utilização da Internet no capítulo IV desta diretiva, no qual o referido artigo 25.° se insere, que visa assegurar o controlo, pelos Estados-Membros, das transferências de dados pessoais para países terceiros e proibir estas transferências quando estes não ofereçam um nível de proteção adequado, não se pode

[47] Este acórdão foi apresentado no Relatório Anual de 2003, p. 67.

presumir que o legislador comunitário tinha a intenção de incluir prospetivamente tal inserção de dados numa página Internet no conceito de «transferência para um país terceiro de dados pessoais», mesmo que deste modo estes dados se tornem acessíveis às pessoas de países terceiros que possuam os meios técnicos para a eles aceder (n.os 63, 64 e 68).

Acórdão de 6 de outubro de 2015 (Grande Secção), Schrems (C-362/14, EU:C:2015:650) [48]

M. Schrems, cidadão austríaco e utilizador da rede social Facebook, apresentou uma queixa no Data Protection Commissioner (Comissário para a proteção de dados, Irlanda) devido ao facto de a Facebook Ireland transferir os dados pessoais dos seus utilizadores para os Estados Unidos e de os conservar em servidores situados naquele país, onde esses dados eram objeto de um tratamento. Segundo M. Schrems, o direito e as práticas dos Estados Unidos não oferecem uma proteção suficiente contra a vigilância por parte das autoridades públicas dos dados transferidos para esse país. O Data Protection Commissioner tinha recusado investigar essa queixa, designadamente pelo facto de, na Decisão 2000/520/CE [49], a Comissão ter considerado que, no contexto do regime denominado «porto seguro» (em inglês «safe harbour») [50], os Estados Unidos asseguravam um nível de proteção adequado aos dados pessoais transferidos.

Foi neste contexto que o Tribunal foi chamado pela High Court (Supremo Tribunal de Justiça, Irlanda) a pronunciar-se sobre um pedido de interpretação do artigo 25.°, n.° 6, da Diretiva 95/46/CE, nos termos do qual a Comissão pode determinar que um país terceiro garante um nível de proteção adequado aos dados transferidos, bem como, em substância, a respeito de um pedido de determinação da validade da Decisão 2000/520 adotada pela Comissão com base no artigo 25.°, n.° 6, da Diretiva 95/46.

O Tribunal declarou a decisão da Comissão inválida no seu conjunto, sublinhando, antes de mais, que a sua adoção exigia a constatação devidamente fundamentada por parte da Comissão de que o país terceiro em causa assegurava efetivamente um nível de proteção dos direitos fundamentais substancialmente equivalente ao garantido na ordem jurídica da União. Ora, na medida em que, na sua Decisão 2000/520, a Comissão não procedeu a essa constatação, o artigo 1.° daquela decisão não cumpre os requisitos estabelecidos no artigo 25.°, n.° 6, da Diretiva 95/46, lido à luz da Carta, sendo por esta razão inválido. Com efeito, os princípios de «porto seguro» só se aplicam às organizações americanas autocertificadas que recebam dados pessoais da União, não sendo exigido que as autoridades públicas americanas estejam sujeitas ao respeito dos referidos princípios. Além do mais, a Decisão 2000/520 possibilitava ingerências nos direitos fundamentais das pessoas cujos dados pessoais eram ou podiam ser transferidos da União para os Estados Unidos, sem conter nenhuma referência à existência, nos Estados Unidos, de regras de natureza estatal destinadas a limitar as eventuais ingerências nesses direitos e sem referir a existência de uma proteção jurídica eficaz contra ingerências desta natureza (n.os 82, 87 a 89, 96 a 98 e disp. 2).

[48] Este acórdão foi apresentado no Relatório Anual de 2015, p. 53.

[49] Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América (JO 2000, L 215, p. 7).

[50] O sistema «porto seguro» inclui um conjunto de princípios relativos à proteção de dados pessoais que as empresas americanas podem subscrever voluntariamente.

Além disso, o Tribunal declarou inválido o artigo 3.° da Decisão 2000/520 na medida em que priva as autoridades nacionais de controlo dos poderes que o artigo 28.° da Diretiva 95/46 lhes conferia nos casos em que uma pessoa apresenta elementos suscetíveis de pôr em causa a compatibilidade com a proteção da vida privada e das liberdades e direitos fundamentais de uma decisão da Comissão que tenha constatado que um país terceiro assegura um nível de proteção adequado (n.os 102 a 104). O Tribunal concluiu que a invalidade dos artigos 1.° e 3.° da Decisão 2000/520 tinha por efeito afetar a validade desta decisão na sua totalidade (n.os 105 e 106).

No que respeita à impossibilidade de justificar tal ingerência, o Tribunal começou por observar que uma regulamentação da União que implique uma ingerência nos direitos fundamentais garantidos pelos artigos 7.° e 8.° da Carta deve prever regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham um mínimo de exigências, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados. A necessidade de dispor destas garantias é ainda mais importante quando os dados pessoais são sujeitos a um tratamento automático e existe um risco significativo de acesso ilícito aos mesmos (n.° 91).

Além disso, e sobretudo, a proteção do direito fundamental ao respeito da vida privada ao nível da União exige que as derrogações à proteção dos dados pessoais e as suas limitações sejam feitas na estrita medida do necessário (n.° 92). Assim, não é limitada ao estritamente necessário uma regulamentação que autoriza de modo generalizado a conservação da totalidade dos dados pessoais de todas as pessoas cujos dados foram transferidos da União para os Estados Unidos sem qualquer diferenciação, limitação ou exceção em função do objetivo prosseguido e sem que esteja previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos, estritamente limitados e suscetíveis de justificar a ingerência que tanto o acesso como a utilização desses dados comportam (n.° 93). Em particular, uma regulamentação que permite às autoridades públicas aceder de forma generalizada ao conteúdo de comunicações eletrónicas infringe o conteúdo essencial do direito fundamental ao respeito pela vida privada. De igual modo, uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a vias de direito para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva, como consagrado no artigo 47.° da Carta (n.os 94 e 95).

Parecer 1/15 (Acordo PNR UE-Canadá) de 26 de julho de 2017 (Grande Secção) (EU:C:2017:592)

Em 26 de julho de 2017, o Tribunal pronunciou-se pela primeira vez sobre a compatibilidade de um projeto de acordo internacional com a Carta dos Direitos Fundamentais da União Europeia, em particular com as disposições relativas ao respeito pela vida privada e à proteção dos dados pessoais.

A União Europeia e o Canadá negociaram um acordo sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros (PNR) que foi assinado em 2014. O Conselho da União Europeia solicitou ao Parlamento Europeu a sua aprovação, tendo este

último decidido recorrer ao Tribunal para saber se o acordo previsto era conforme com o direito da União.

O projeto de acordo permite a transferência sistemática e contínua dos dados PNR de todos os passageiros a uma autoridade canadiana para a utilização e o armazenamento, bem como a sua eventual transferência ulterior para outras autoridades e outros países terceiros, com vista a lutar contra o terrorismo e a criminalidade transnacional grave. Para esse efeito, o projeto de acordo prevê, nomeadamente, um período de cinco anos de conservação dos dados e prevê exigências especiais em matéria de segurança e integridade dos PNR, tal como a ocultação imediata dos dados sensíveis, e prevê direitos de acesso, de retificação e de supressão bem como a possibilidade interpor recursos administrativos ou judiciais.

Os dados PNR visados pelo acordo previsto incluem, designadamente, além do nome e dos elementos de contacto do passageiro ou dos passageiros, informações necessárias à reserva, tais como as datas previstas da viagem e o respetivo itinerário, informações sobre os bilhetes, os grupos de pessoas registadas sob o mesmo número de reserva, informações relativas aos meios de pagamento ou à faturação, informações sobre as bagagens e observações gerais acerca dos passageiros.

No seu parecer, o Tribunal declarou que o acordo PNR não pode ser celebrado na sua forma atual devido à incompatibilidade de várias das suas disposições com os direitos fundamentais reconhecidos pela União.

O Tribunal declarou, em primeiro lugar, que tanto a transferência dos dados PNR da União para a autoridade canadiana competente como o enquadramento negociado pela União com o Canadá das condições respeitantes ao período de conservação desses dados, à sua utilização e à sua transferência ulterior para outras autoridades canadianas, à Europol, ao Eurojust, às autoridades policiais ou judiciais dos Estados-Membros ou ainda às autoridades de outros países terceiros, constituem uma ingerência no direito garantido pelo artigo 7.° da Carta. Estas operações são igualmente constitutivas de uma ingerência no direito fundamental à proteção dos dados pessoais garantido pelo artigo 8.° da Carta, visto que constituem tratamentos dos dados pessoais (n.os 125 e 126).

Além disso, o Tribunal sublinhou que, embora alguns dos dados PNR, tomados isoladamente, não pareçam suscetíveis de revelar informações importantes sobre a vida privada das pessoas em causa, o certo é que, considerados conjuntamente, os referidos dados podem, entre outros, revelar um itinerário de viagem completo, hábitos de viagem, relações existentes entre duas ou mais pessoas e informações sobre a situação financeira dos passageiros aéreos, os seus hábitos alimentares ou o seu estado de saúde, podendo até fornecer informações sensíveis sobre esses passageiros, conforme definidas no artigo 2.°, alínea e), do acordo projetado (informações que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas, etc.) (n.° 128).

A este respeito, o Tribunal considerou que, embora as intervenções em causa possam ser justificadas pela prossecução de um objetivo de interesse geral (garantia da segurança pública no âmbito da luta contra as infrações terroristas e a criminalidade transnacional grave), várias disposições do Acordo não são limitadas ao estritamente necessário e não preveem regras claras e precisas.

Em especial, o Tribunal salientou que, tendo em conta o risco de um tratamento contrário ao princípio da não discriminação, a transferência de dados sensíveis para o Canadá exigiria uma justificação precisa e particularmente sólida, baseada em fundamentos diferentes da proteção da segurança pública contra o terrorismo e a criminalidade transnacional grave. Ora, neste caso, tal justificação não existe. O Tribunal concluiu que as disposições do acordo sobre a transferência de dados sensíveis para o Canadá, bem como sobre o tratamento e a conservação desses dados são incompatíveis com os direitos fundamentais (n.os 165 e 232).

Em segundo lugar, o Tribunal considerou que, após a partida dos passageiros aéreos do Canadá, o armazenamento contínuo dos dados PNR de todos os passageiros aéreos permitido pelo acordo projetado não se limita ao estritamente necessário. Com efeito, no que se refere aos passageiros aéreos em relação aos quais, à sua chegada ao Canadá e até à sua saída deste país, não foi identificado um risco em matéria de terrorismo ou criminalidade transnacional grave, não se afigura existir, uma vez saídos desse país, nenhuma relação, ainda que indireta, entre os seus dados PNR e o objetivo prosseguido pelo acordo projetado, que justifique a conservação destes dados. Em contrapartida, o armazenamento dos dados PNR relativos a passageiros aéreos relativamente aos quais são identificados elementos objetivos que permitem considerar que, mesmo após a sua partida do Canadá, os mesmos podem apresentar um risco em termos de luta contra o terrorismo e a criminalidade transnacional grave é admissível para além da sua estada nesse país, mesmo por um período de cinco anos (n.os 205 a 207 e 209).

Em terceiro lugar, o Tribunal declarou que o direito fundamental ao respeito pela vida privada, consagrado no artigo 7.° da Carta dos Direitos Fundamentais da União Europeia, implica que a pessoa em causa possa certificar-se de que esses dados pessoais são tratados com exatidão e de forma lícita. Para poder efetuar as verificações necessárias, essa pessoa deve dispor de um direito de acesso aos dados que lhe digam respeito que são objeto de um tratamento.

A este respeito, o Tribunal sublinhou que, no acordo projetado, importa que os passageiros aéreos sejam informados da transferência dos seus dados dos registos de identificação dos passageiros para o país terceiro em causa e da utilização de tais dados a partir do momento em que essa comunicação não seja suscetível comprometer as investigações levadas a cabo pelas autoridades públicas a que se aplica o acordo projetado. Com efeito, essa informação é, de facto, necessária para permitir aos passageiros aéreos exercer os seus direitos de pedir o acesso aos dados que lhes dizem respeito e, sendo caso disso, a retificação dos mesmos, bem como intentar, em conformidade com o artigo 47.°, primeiro parágrafo, da Carta, uma ação perante um tribunal.

Assim, nas hipóteses em que existem elementos objetivos que justificam a utilização dos dados dos registos de identificação dos passageiros para lutar contra o terrorismo e a criminalidade transnacional grave e que carecem de uma autorização prévia de uma autoridade judiciária ou de uma entidade administrativa independente, afigura-se necessária uma informação individual dos passageiros. O mesmo se diga dos casos em que os dados PNR dos passageiros aéreos são comunicados a outras autoridades públicas ou a particulares. No entanto, tal informação apenas deve ocorrer a partir do momento em que não seja suscetível de comprometer as investigações levadas a cabo pelas autoridades públicas previstas no acordo projetado (n.os 219, 220, 223 e 224).

Acórdão de 16 de julho de 2020 (Grande Secção), Facebook Ireland et Schrems (C-311/18, EU:C:2020:559) [51]

O RGPD dispõe que a transferência de dados pessoais para um país terceiro só pode, em princípio, ter lugar, se o país terceiro em questão assegurar um nível de proteção adequado desses dados. Segundo esse regulamento, a Comissão pode constatar que um país terceiro assegura, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção adequado [52]. Na falta de tal decisão de adequação, essa transferência só pode ser realizada se o exportador dos dados pessoais, estabelecido na União, previr garantias adequadas, que podem nomeadamente resultar de cláusulas-tipo de proteção de dados adotadas pela Comissão, e se as pessoas em causa dispuserem de direitos oponíveis e de vias efetivas de recurso [53]. Por outro lado, o RGPD prevê, de forma precisa, as condições em que essa transferência pode ocorrer, na falta de uma decisão de adequação ou de garantias adequadas [54].

Maximillian Schrems, nacional austríaco residente na Áustria, é utilizador do Facebook desde 2008. Como para os demais utilizadores que residem na União, os dados pessoais de M. Schrems são, no todo ou em parte, transferidos pela Facebook Ireland para servidores que pertencem à Facebook Inc., situados no território dos Estados Unidos, país em que são objeto de tratamento. M. Schrems apresentou uma queixa à autoridade irlandesa de controlo na qual requeria, em substância, que essas transferências fossem proibidas. Sustentou que o direito e as práticas dos Estados Unidos não oferecem proteção suficiente contra o acesso aos dados transferidos para esse país por parte das autoridades públicas. Esta queixa foi indeferida, com o fundamento, nomeadamente, de que a Comissão, na sua Decisão 2000/520 [55], tinha constatado que os Estados Unidos asseguravam um nível de proteção adequado. Por acórdão proferido em 6 de outubro de 2015, o Tribunal, chamado a pronunciar-se sobre uma questão prejudicial submetida pela High Court (Tribunal Superior, Irlanda), declarou esta decisão inválida (a seguir «acórdão Schrems I») [56] (n.os 52 e 53).

Na sequência do acórdão Schrems I e da consequente anulação da decisão de indeferimento da queixa de M. Schrems por parte do órgão jurisdicional irlandês, a autoridade de controlo irlandesa convidou-o a reformular a sua queixa tendo em conta a declaração de invalidade da Decisão 2000/520 por parte do Tribunal. Na queixa reformulada, M. Schrems reafirma que os Estados Unidos não oferecem uma proteção suficiente dos dados transferidos para esse país. Pede que, no futuro, sejam suspensas ou proibidas as transferências desses dados pessoais a partir da União para os Estados Unidos, que a Facebook Ireland passou a realizar com fundamento nas cláusulas-tipo de proteção que figuram no anexo da Decisão 2010/87/UE [57]. Considerando que o tratamento da queixa de M. Schrems dependia, nomeadamente, da validade da Decisão 2010/87, a autoridade de controlo irlandesa deu início a um processo na

---

51 Este acórdão foi apresentado no Relatório Anual de 2020, pp. 26 a 29.

52 Artigo 45.º do RGPD.

53 Artigo 46.º, n.os 1 e 2, alínea c), do RGPD.

54 Artigo 49.º do RGPD.

55 Decisão da Comissão de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América (JO 2000, L 215, p. 7).

56 Acórdão do Tribunal de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650 (v. igualmente CI n.º 117/15).

57 Decisão da Comissão, de 5 de fevereiro de 2010, relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho (JO 2010, L 39, p. 5), conforme alterada pela Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de dezembro de 2016 (JO 2016, L 344, p. 100).

High Court com vista a que esta apresentasse um pedido prejudicial no Tribunal. Posteriormente à abertura deste processo, a Comissão adotou a Decisão (UE) 2016/1250 relativa à adequação da proteção assegurada pelo Escudo de Proteção da Privacidade UE-Estados Unidos [58] (n.os 54, 55 e 57).

Através do seu pedido de decisão prejudicial, o órgão jurisdicional de reenvio interroga o Tribunal sobre a aplicabilidade do RGPD a transferências de dados pessoais com fundamento nas cláusulas-tipo de proteção que figuram na Decisão 2010/87, a respeito do nível de proteção exigido por este regulamento no quadro dessa transferência e a respeito das obrigações que incumbem às autoridades de controlo nesse contexto. A High Court suscitou ainda a questão da validade da Decisão 2010/87 e da Decisão 2016/1250.

No seu acórdão, o Tribunal constata que a análise da Decisão 2010/87 à luz da Carta não revelou nenhum elemento suscetível de afetar a sua validade. Em contrapartida, o Tribunal declarou a Decisão 2016/1250 inválida (disp. 4 e 5).

O Tribunal considera, antes de mais, que o direito da União, nomeadamente o RGPD, é aplicável a uma transferência de dados pessoais efetuada para fins comerciais por um operador económico estabelecido num Estado-Membro para outro operador económico estabelecido num país terceiro, não obstante o facto de, no decurso ou na sequência dessa transferência, esses dados serem suscetíveis de ser tratados pelas autoridades do país terceiro em causa para efeitos de segurança pública, de defesa e de segurança do país terceiro em causa. O Tribunal precisou que este tipo de tratamento de dados pelas autoridades de um país terceiro não pode excluir essa transferência do âmbito de aplicação do RGPD (n.os 86, 88, 89 e disp. 1).

No que diz respeito ao nível de proteção exigido no contexto de tal transferência, o Tribunal declara que as exigências previstas para o efeito pelas disposições do RGPD, relacionadas com garantias adequadas, direitos oponíveis e vias de recurso efetivas, devem ser interpretadas no sentido de que as pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas tipo de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União por este regulamento, lido à luz da Carta. Neste contexto, o Tribunal precisa que a avaliação desse nível de proteção deve ter em consideração tanto as estipulações contratuais acordadas entre o exportador de dados estabelecido na União e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país (n.º 105 e disp. 2).

Quanto às obrigações que incumbem às autoridades de controlo no contexto dessa transferência, o Tribunal declara que, a menos que exista uma decisão de adequação validamente adotada pela Comissão, essas autoridades estão nomeadamente obrigadas a suspender ou a proibir uma transferência de dados para um país terceiro, se considerarem, à luz de todas as circunstâncias específicas dessa transferência, que essas cláusulas tipo de proteção de dados não são ou não podem ser respeitadas nesse país e que a proteção dos dados transferidos exigida pelo direito da União não pode ser assegurada por outros meios, no

[58] Decisão de Execução da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho (JO 2016, L 207, p. 1).

caso de o exportador estabelecido na União não ter ele próprio suspendido ou posto termo a essa transferência (n.° 121 e disp. 3).

Em seguida, o Tribunal analisa a validade da Decisão 2010/87. Segundo o Tribunal, a validade desta decisão não é posta em causa pelo simples facto de as cláusulas-tipo de proteção de dados que nela figuram não vincularem, devido à sua natureza contratual, as autoridades do país terceiro para o qual a transferência pode ser efetuada. Em contrapartida, o Tribunal precisa que esta validade depende da questão de saber se a referida decisão inclui mecanismos efetivos que permitam, na prática, assegurar que o nível de proteção exigido pelo direito da União seja respeitado e que as transferências de dados pessoais, fundadas nessas cláusulas, sejam suspensas ou proibidas em caso de violação dessas cláusulas ou de impossibilidade de as respeitar. O Tribunal constata que a Decisão 2010/87 cria esses mecanismos. A este respeito, sublinha, nomeadamente, que esta decisão instaura uma obrigação de o exportador de dados e o destinatário da transferência verificarem, previamente, se esse nível de proteção é respeitado no país terceiro em causa e que obriga esse destinatário a informar o exportador de dados da sua eventual incapacidade de dar cumprimento às cláusulas tipo de proteção, incumbindo então a este último suspender a transferência de dados e/ou resolver o contrato celebrado com o primeiro (n.os 132, 136, 137, 142, 148 e disp. 4).

Por último, o Tribunal procede à análise da validade da Decisão 2016/1250 tendo em conta as exigências decorrentes do RGPD, lido à luz das disposições da Carta que garantem o respeito da vida privada e familiar, a proteção de dados pessoais e o direito a uma proteção jurisdicional efetiva. A este respeito, o Tribunal observa que, à semelhança da Decisão 2000/520, esta decisão consagra o primado das exigências relativas à segurança nacional, ao interesse público e ao respeito da legislação americana, tornando assim possíveis ingerências nos direitos fundamentais das pessoas cujos dados são transferidos para esse país terceiro. Segundo o Tribunal, as limitações da proteção de dados pessoais que decorrem da regulamentação interna dos Estados Unidos relativa ao acesso e à utilização, pelas autoridades públicas americanas, desses dados transferidos a partir da União, para esse país terceiro, e que a Comissão avaliou na Decisão 2016/1250, não são enquadrados de forma a satisfazer os requisitos substancialmente equivalentes aos exigidos, no direito da União, pelo princípio da proporcionalidade, na medida em que os programas de vigilância que assentam nessa regulamentação não se limitam ao estritamente necessário. Baseando-se nas conclusões desta decisão, o Tribunal observa que, relativamente a certos programas de vigilância, não resulta de forma alguma da referida regulamentação que existam limitações à habilitação nela prevista para a execução de tais programas nem que existam garantias para nacionais não americanos potencialmente visados. O Tribunal acrescenta que, embora essa regulamentação preveja requisitos que as autoridades americanas devem respeitar quando executam os programas de vigilância em causa, a mesma não confere aos cidadãos direitos oponíveis às autoridades americanas nos tribunais (n.os 164, 165, 180-182, 184, 185).

Quanto à exigência de proteção jurisdicional, o Tribunal declara que, contrariamente ao que a Comissão entendeu na Decisão 2016/1250, o mecanismo de mediação visado por esta decisão não fornece a essas pessoas uma via de recurso perante um órgão que ofereça garantias substancialmente equivalentes às exigidas pelo direito da União e que sejam suscetíveis de assegurar quer a independência do mediador prevista por esse mecanismo quer a existência de normas que habilitem esse mediador a tomar decisões vinculativas relativamente aos

serviços de informações americanos. Com fundamento em todas estas razões, o Tribunal declarou a Decisão 2016/1250 inválida (n.os 195-197, 201 e disp. 5).

V. Proteção dos dados pessoais na Internet

1. Direito de oposição ao tratamento dos dados pessoais («direito a ser esquecido»)

Acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, EU:C:2014:317)

Neste acórdão (ver também rubrica II.3, intitulada «Conceito de 'tratamento de dados pessoais'»), o Tribunal precisou o alcance dos direitos de acesso e de oposição ao tratamento de dados pessoais na Internet, previstos pela Diretiva 95/46.

Assim, quando se pronunciou sobre a questão do alcance da responsabilidade do operador de um motor de busca na Internet, o Tribunal declarou, em substância, que, para respeitar os direitos de acesso e oposição garantidos pelos artigos 12.°, alínea b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46/CE, e desde que as condições previstas nesses artigos estejam reunidas, este é, em certas circunstâncias, obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a páginas *web* publicadas por terceiros e que contenham informações sobre essa pessoa. O Tribunal precisou que essa obrigação também pode existir na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas *web*, isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita (n.° 88 e disp. 3).

Por outro lado, interrogado sobre a questão de saber se a diretiva permite que a pessoa em causa solicite que ligações a páginas web sejam suprimidas de uma lista de resultados com o fundamento de que pretende que as informações que aí figuram relativas à sua pessoa sejam «esquecidas» após um certo período de tempo, o Tribunal salienta, em primeiro lugar, que mesmo um tratamento inicialmente lícito de dados exatos se pode tornar, com o tempo, incompatível com esta diretiva, quando esses dados já não sejam necessários atendendo às finalidades para que foram recolhidos ou tratados, designadamente, quando são objetivamente inadequados, quando não são pertinentes ou já não são pertinentes ou quando são excessivos atendendo a essas finalidades ou ao tempo decorrido (n.° 93). Assim, caso se conclua, no seguimento de um pedido da pessoa em causa, que a inclusão dessas ligações na lista é, na situação atual, incompatível com a diretiva, as informações e ligações que figuram nesta lista devem ser suprimidas (n.° 94). Neste contexto, a constatação de um direito da pessoa em causa a que a informação sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados não pressupõe que a inclusão da informação em questão na lista de resultados cause prejuízo à pessoa em causa (n.° 96 e disp. 4).

Por último, o Tribunal indicou que, na medida em que a pessoa em causa pode, tendo em conta os seus direitos fundamentais ao abrigo dos artigos 7.° e 8.° da Carta, requerer que a

informação em questão deixe de estar à disposição do grande público através da sua inclusão numa lista de resultados deste tipo, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em encontrar a referida informação durante uma pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais, como o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão em virtude dessa inclusão (n.° 97 e disp. 4).

2. Tratamento dos dados pessoais e direitos de propriedade intelectual

Acórdão de 29 de janeiro de 2008 (Grande Secção), Promusicae (C-275/06, EU:C:2008:54) [59]

A Promusicae, uma associação espanhola sem fins lucrativos que agrupa produtores e editores de gravações musicais e audiovisuais, tinha recorrido aos tribunais espanhóis para que a Telefónica de España SAU (sociedade comercial que tem como atividade, nomeadamente, a prestação de serviços de acesso à Internet) fosse intimada a revelar a identidade e o endereço físico de certas pessoas a quem esta última prestava serviços de acesso à Internet e cujo endereço IP e a data e hora da ligação eram conhecidas. Segundo a Promusicae, essas pessoas utilizavam o programa de troca de ficheiros dito «peer-to-peer» ou «P2P» (meio transparente de partilha de conteúdos, independente, descentralizado e munido de funções de busca e de descarga avançadas) e permitiam o acesso, nos ficheiros partilhados dos respetivos computadores pessoais, a fonogramas cujos direitos patrimoniais de exploração pertenciam aos sócios da Promusicae. Assim, pedia que lhe fossem transmitidas essas informações para poder propor ações cíveis contra os interessados.

Nestas condições, o Juzgado de lo Mercantil n.° 5 de Madrid (Tribunal de Comércio n.° 5 de Madrid, Espanha) submeteu ao Tribunal a questão de saber se a legislação europeia impõe aos Estados-Membros que prevejam, para garantir a efetiva proteção dos direitos de autor, a obrigação de transmitir dados de caráter pessoal no âmbito de uma ação cível.

Segundo o Tribunal, o referido pedido de decisão prejudicial suscitou a questão da necessária conciliação entre as exigências ligadas à proteção de diferentes direitos fundamentais, a saber, por um lado, o direito ao respeito pela vida privada, e, por outro, os direitos à proteção da propriedade e a uma tutela jurisdicional efetiva.

A este respeito, o Tribunal concluiu que as Diretivas 2000/31/CE, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») [60], 2001/29/CE, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação [61],

[59] Este acórdão foi apresentado no Relatório Anual de 2008, p. 46.

[60] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO 2000, L 178, p. 1).

[61] Diretiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de maio de 2001, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação (JO 2001, L 167, p. 10).

2004/48/CE, relativa ao respeito dos direitos de propriedade intelectual [62], e 2002/58, não impõem aos Estados-Membros que prevejam, numa situação como a do processo principal, a obrigação de transmitir dados pessoais para garantir a efetiva proteção dos direitos de autor no âmbito de uma ação cível. Porém, o direito da União exige que os referidos Estados, na transposição dessas diretivas, providenciem no sentido de ser seguida uma interpretação das mesmas que permita assegurar um justo equilíbrio entre os direitos fundamentais protegidos pela ordem jurídica comunitária. Em seguida, ao darem execução às medidas de transposição das referidas diretivas, incumbe às autoridades e aos órgãos jurisdicionais dos Estados-Membros não apenas interpretar o seu direito nacional em conformidade com essas mesmas diretivas, mas também seguir uma interpretação destas que não entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito comunitário, como o princípio da proporcionalidade (n.° 70 e disp.).

Acórdão de 24 de novembro de 2011, Scarlet Extended (C-70/10, EU:C:2011:771) [63]

A sociedade belga de autores, compositores e editores SCRL (SABAM) constatou que os internautas que utilizam os serviços da Scarlet Extended SA, um fornecedor de acesso à Internet (a seguir «Scarlet»), descarregavam na Internet, sem autorização e sem pagar direitos, obras constantes do seu catálogo através de redes «peer-to-peer». A SABAM intentou uma ação no tribunal nacional, o qual, em primeira instância, julgou procedente a sua pretensão e intimou a Scarlet a pôr termo a essas violações dos direitos de autor tornando impossível, através de um *software* «peer-to-peer», qualquer forma de envio ou de receção pelos seus clientes de ficheiros eletrónicos contendo uma obra musical do repertório da SABAM.

Chamada a conhecer do processo pela Scarlet, a cour d'appel de Bruxelles (Tribunal de Recurso de Bruxelas, Bélgica) suspendeu a instância para perguntar ao Tribunal de Justiça, a título prejudicial, se tal medida inibitória era compatível com o direito europeu.

O Tribunal declarou que as Diretivas 95/46, 2000/31, 2001/29, 2002/58 e 2004/48, lidas conjuntamente e interpretadas à luz das exigências resultantes da proteção dos direitos fundamentais aplicáveis, devem ser interpretadas no sentido de que se opõem a uma medida inibitória que intima a Scarlet a criar um sistema de filtragem de todas as comunicações eletrónicas que transitam pelos seus serviços, nomeadamente através da utilização de *software* «peer-to-peer», aplicável indistintamente a toda a sua clientela, com caráter preventivo, a expensas suas e sem limitação no tempo, e que seja apta a identificar na rede desse fornecedor a circulação de ficheiros eletrónicos que contenham uma obra musical, cinematográfica ou audiovisual sobre a qual o requerente alega ser titular de direitos de propriedade intelectual, com o objetivo de bloquear a transferência de ficheiros cujo intercâmbio viole os direitos de autor (n.° 54 e disp.).

Com efeito, segundo o Tribunal, uma tal medida inibitória não respeita a proibição, imposta pelo artigo 15.°, n.° 1, da Diretiva 2000/31, de impor a esse prestador de serviços uma obrigação geral de vigilância, nem a exigência de assegurar o justo equilíbrio entre, por um lado, o direito

[62] Diretiva 2004/48/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao respeito dos direitos de propriedade intelectual (JO 2004, L 157, p. 45, e retificação no JO 2004, L 195, p. 16);

[63] Este acórdão foi apresentado no Relatório Anual de 2011, p. 37.

de propriedade intelectual e, por outro, a liberdade de empresa e o direito à proteção dos dados pessoais, bem como a liberdade de receber ou de transmitir informações (n.os 40,49).

Neste contexto, o Tribunal salientou que, por um lado, a medida inibitória que ordena a instalação do sistema de filtragem controvertido implicaria uma análise sistemática de todos os conteúdos e a recolha e identificação dos endereços IP dos utilizadores que estão na origem do envio de conteúdos ilícitos na rede, sendo esses endereços dados pessoais protegidos, uma vez que permitem a identificação precisa dos referidos utilizadores. Por outro lado, haveria o risco de a referida medida inibitória violar a liberdade de informação, dado que esse sistema poderia não distinguir suficientemente um conteúdo ilícito de um lícito, de modo que o seu acionamento poderia provocar o bloqueio de comunicações de conteúdo lícito. Com efeito, não é contestado que a resposta à questão da licitude de uma transmissão depende igualmente da aplicação de exceções legais aos direitos de autor que variam de um Estado-Membro para outro. Além disso, em certos Estados-Membros, certas obras podem pertencer ao domínio público ou os autores em causa podem colocá-las gratuitamente à disposição do público na Internet (n.° 52).

Consequentemente, o Tribunal declarou que, ao adotar a medida inibitória que obriga a Scarlet a instalar o sistema de filtragem controvertido, o órgão jurisdicional nacional não respeitou a exigência de assegurar um justo equilíbrio entre o direito de propriedade intelectual, por um lado, e a liberdade de empresa, o direito à proteção dos dados pessoais e a liberdade de receber ou de enviar informações, por outro (n.° 53).

Acórdão de 19 de abril de 2012, Bonnier Audio e o. (C-461/10, EU:C:2012:219)

O Högsta domstolen (Supremo Tribunal, Suécia) submeteu um pedido prejudicial ao Tribunal com vista à interpretação das Diretivas 2002/58/CE e 2004/48/CE, no âmbito de um litígio que opõe a Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB e a Storyside AB (a seguir «Bonnier Audio e o.») à Perfect Communication Sweden AB (a seguir «ePhone») a respeito da oposição desta última a um pedido de injunção para comunicação de dados apresentado pela Bonnier Audio e o.

No caso em apreço, a Bonnier Audio e o. eram sociedades editoras, titulares, nomeadamente, de direitos exclusivos de reprodução, edição e colocação à disposição do público de 27 obras que se apresentavam sob a forma de audiolivros. Consideravam que os seus direitos exclusivos tinham sido violados devido à difusão ao público dessas 27 obras, sem o seu consentimento, por meio de um servidor FTP («file transfer protocol») que permitia a partilha de ficheiros e a transmissão de dados entre computadores ligados à Internet. Por conseguinte, apresentaram aos tribunais suecos um pedido de injunção para comunicação do nome e endereço da pessoa que utilizava o endereço IP a partir do qual se presumia que os ficheiros em causa tinham sido transmitidos.

Neste contexto, o Högsta domstolen, chamado a conhecer do recurso, interrogou o Tribunal sobre a questão de saber se o direito da União obsta à aplicação de uma disposição nacional adotada com base no artigo 8.° da Diretiva 2004/48 que, com o objetivo de identificar um assinante, permite que se imponha a um fornecedor de Internet a obrigação de comunicar ao titular de um direito de autor, ou aos seus sucessores, no âmbito de um processo civil, a

identidade do assinante a quem foi atribuído um endereço IP e a partir do qual foi praticada a violação do referido direito. A questão pressupunha, por um lado, que o requerente da injunção tinha reunido indícios reais de violação de um direito de autor e, por outro lado, que a medida era proporcionada.

O Tribunal começou por recordar que o artigo 8.°, n.° 3, da Diretiva 2004/48, lido em conjugação com o artigo 15.°, n.° 1, da Diretiva 2002/58, não se opõe a que os Estados-Membros prevejam uma obrigação de transmissão de dados pessoais a entidades privadas a fim de permitir desencadear, nas instâncias cíveis, um procedimento judicial contra as violações dos direitos de autor, mas também não obriga esses Estados a prever essa obrigação. No entanto, incumbe às autoridades e aos órgãos jurisdicionais dos Estados-Membros não só interpretar o seu direito nacional em conformidade com estas mesmas diretivas mas também providenciar no sentido de ser seguida uma interpretação destas que não entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito da União, como o princípio da proporcionalidade (n.os 55 e 56).

A este respeito, foi constatado que a legislação nacional em questão exigia, nomeadamente, que, para que pudesse ser ordenada uma intimação de comunicação dos dados em causa, existissem indícios reais de violação de um direito de propriedade intelectual sobre uma obra, que as informações pedidas fossem suscetíveis de facilitar a investigação sobre a violação do direito de autor ou a lesão desse direito e que as razões que justificavam essa intimação fossem de interesse superior aos inconvenientes ou aos outros prejuízos que a mesma pudesse ocasionar ao seu destinatário ou a qualquer interesse que se lhe opusesse (n.° 58).

Por conseguinte, o Tribunal concluiu que as Diretivas 2002/58 e 2004/48 não se opõem a uma legislação nacional como a que estava em causa no processo principal, na medida em que esta legislação permite ao órgão jurisdicional nacional ao qual uma pessoa com legitimidade ativa apresentou um pedido de intimação para comunicação de dados pessoais, ponderar os interesses opostos envolvidos em função das circunstâncias de cada caso e tendo em devida conta as exigências decorrentes do princípio da proporcionalidade (n.° 61 e disp).

Acórdão de 17 de junho de 2021, M.I.C.M. (C-597/19, EU:C:2021:492)

A empresa Mircom International Content Management & Consulting (M.I.C.M.) Limited (a seguir «Mircom») apresentou um pedido de informação contra a Telenet BVBA, um fornecedor de acesso à Internet, no Ondernemingsrechtbank Antwerpen (Tribunal do Comércio de Antuérpia, Bélgica, a seguir «órgão jurisdicional de reenvio»). Esse pedido destina-se a obter uma decisão que obrigue a Telenet a apresentar os dados de identificação dos seus clientes com base nos endereços IP recolhidos por uma sociedade especializada, por conta da Mircom. As ligações Internet de clientes da Telenet foram utilizadas para partilhar filmes que fazem parte do catálogo da Mircom, numa rede descentralizada (*peer-to-peer*), com recurso ao protocolo *BitTorrent*. A Telenet contesta o pedido da Mircom.

Foi neste contexto que o órgão jurisdicional de reenvio perguntou ao Tribunal de Justiça, em primeiro lugar, se a partilha, na referida rede, de segmentos de um ficheiro multimédia que contém uma obra protegida constitui uma comunicação ao público ao abrigo do direito da União. Em seguida, o órgão jurisdicional de reenvio pretende saber se o titular de direitos de

propriedade intelectual, como a Mircom, que não os utiliza, mas que reclama indemnizações a pretensos infratores, pode beneficiar das medidas, procedimentos e recursos previstos pelo direito da União para assegurar o respeito desses direitos, por exemplo, pedindo informações. Por último, o órgão jurisdicional de reenvio convidou o Tribunal a clarificar a questão da licitude, por um lado, da forma como os endereços IP dos clientes foram recolhidos pela Mircom e, por outro, da comunicação dos dados pedida pela Mircom à Telenet.

O Tribunal declara que o direito da União [64] não se opõe, em princípio, nem ao registo sistemático, pelo titular de direitos de propriedade intelectual ou por um terceiro por sua conta, de endereços IP de utilizadores de redes descentralizadas (*peer-to-peer*) cujas ligações à Internet foram pretensamente utilizadas em atividades ilícitas (tratamento de dados a montante) nem à comunicação dos nomes e dos endereços postais desses utilizadores a esse titular ou a um terceiro para efeitos de uma ação de indemnização (tratamento de dados a jusante). Todavia, as iniciativas e os pedidos a este respeito devem ser justificados, proporcionados, não abusivos e previstos por uma medida legislativa nacional que restrinja o âmbito dos direitos e das obrigações decorrentes do direito da União. O Tribunal precisa que este último não estabelece a obrigação de uma sociedade, como a Telenet, comunicar a pessoas privadas os dados pessoais a fim de permitir intentar, em instâncias cíveis, processos contra violações dos direitos de autor. O direito da União permite, no entanto, que os Estados Membros imponham essa obrigação (n.os 97, 125 a 127 e disp. 3).

3. Supressão de referências a dados pessoais

Acórdão de 24 de setembro de 2019 (Grande Secção), GC e o. (Supressão de referências a dados sensíveis) (C-136/17, EU:C:2019:773) [65]

Neste acórdão, o Tribunal, reunido em Grande Secção, precisou as obrigações do operador de um motor de busca no quadro de um pedido de supressão de dados sensíveis.

A Google tinha rejeitado os pedidos de quatro pessoas no sentido de serem suprimidas da lista de resultados exibida pelo motor de busca em resposta a uma pesquisa efetuada a partir dos respetivos nomes, diversas hiperligações que conduziam a páginas web publicadas por terceiros, nomeadamente a artigos de imprensa. Na sequência das queixas dessas quatro pessoas, a Commission nationale de l'informatique et des libertés (Comissão Nacional da Informática e das Liberdades, CNIL, França) indeferiu o pedido para que a Google fosse intimada a proceder às supressões de referências pedidas. O Conseil d'État (França), chamado a pronunciar-se, pediu ao Tribunal que precisasse as obrigações que incumbem ao operador de um motor de busca aquando do tratamento de um pedido de supressão de referências ao abrigo da Diretiva 95/46.

Em primeiro lugar, o Tribunal recordou que é proibido o tratamento dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual [66], sob reserva de algumas exceções e derrogações. No que diz respeito ao tratamento de dados

[64] Artigo 6.º, n.º 1, alínea f), do RGPD, e artigo 15.º, n.º 1, da Diretiva 2002/58.
[65] Este acórdão foi apresentado no Relatório Anual de 2019, pp. 117 e 118.
[66] Artigo 8, n.º 1, da Diretiva 95/46/CE e artigo 9.º, 1, do Regulamento 2016/679.

relativos a infrações, a condenações penais ou a medidas de segurança, em princípio o tratamento só poderá ser efetuado sob o controlo das autoridades públicas ou se o direito nacional estabelecer garantias adequadas e específicas [67] (n.os 39 e 40).

O Tribunal declarou que a proibição e as restrições relativas ao tratamento dessas categorias particulares de dados se aplicam a um operador de um motor de busca, à semelhança de qualquer outro responsável pelo tratamento de dados pessoais. Com efeito, a finalidade dessas proibições e restrições consiste em assegurar uma maior proteção contra tais tratamentos, que, devido à sensibilidade específica desses dados, podem constituir uma ingerência especialmente grave nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais (n.os 42 a 44).

Todavia, o operador de um motor de busca não é responsável pelo facto de, numa página web publicada por um terceiro, figurarem dados pessoais, mas sim pelo facto de referenciar essa página. Nestas condições, as proibições e restrições relativas ao tratamento de dados sensíveis apenas se aplicam a este operador devido a essas referências e, por conseguinte, por intermédio de uma verificação a efetuar, sob o controlo das autoridades nacionais competentes, com base num pedido apresentado pela pessoa em causa (n.os 46 e 47).

Em segundo lugar, o Tribunal considerou que, perante um pedido de supressão de referências a dados sensíveis, em princípio o operador é obrigado, sob reserva de certas exceções, a acolher este pedido. No que respeita a tais exceções, o operador pode, nomeadamente, recusar o referido pedido quando constatar que as hiperligações conduzem a dados que foram manifestamente tornados públicos pela pessoa em causa [68], desde que as referências a essas hiperligações cumpram os outros requisitos de licitude de um tratamento de dados pessoais e desde que essa pessoa não tenha o direito de se opor a essas referências por razões relacionadas com a sua situação particular [69] (n.os 65 e 69).

Em qualquer caso, perante um pedido de supressão de referências, o operador de um motor de busca deve verificar se a inclusão na lista de resultados de uma hiperligação para uma página web na qual são publicados dados sensíveis, que é exibida após uma pesquisa efetuada a partir do nome dessa pessoa, é estritamente necessária para proteger a liberdade de informação dos internautas potencialmente interessados em aceder a essa página web através dessa pesquisa. A este respeito, o Tribunal sublinhou que, embora os direitos ao respeito da vida privada e à proteção de dados pessoais, regra geral, prevaleçam sobre a liberdade de informação dos internautas, este equilíbrio pode, todavia, depender, em casos particulares, da natureza da informação em questão e da sua sensibilidade para a vida privada da pessoa em causa, bem como do interesse do público em dispor dessa informação, que pode variar, designadamente, em função do papel desempenhado por essa pessoa na vida pública (n.os 66 e 68).

Em terceiro lugar, o Tribunal declarou que, no contexto de um pedido de supressão das referências a dados relativos a um processo judicial em matéria penal, em que a pessoa em causa era arguida, e que respeitam a uma fase anterior desse processo e já não correspondem à situação atual, atendendo a todas as circunstâncias do caso concreto, como, nomeadamente,

[67] Artigo 8.°, n.° 5, da Diretiva 95/46/CE e artigo 10..° do Regulamento 2016/679.
[68] Artigo 8.°, n.° 2, alínea e), da Diretiva 95/46/CE e artigo 9.°, n.° 2, alínea e) do Regulamento 2016/679..
[69] Artigo 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46/CE e artigo 21.°, n.° 1, do Regulamento 2016/679.

a natureza e a gravidade da infração em questão, o desenrolar e o resultado final do processo, o tempo decorrido, o papel desempenhado por essa pessoa na vida pública e o seu comportamento no passado, o interesse do público no momento em que o pedido é apresentado, o conteúdo e a forma da publicação, bem como as repercussões desta para a referida pessoa, esta última tem direito a que as informações em questão já não estejam, no momento atual, associadas ao seu nome através de uma lista de resultados, exibida após uma pesquisa efetuada a partir desse nome. No entanto, mesmo que tal não seja o caso devido ao facto de a inclusão da hiperligação em causa se revelar estritamente necessária para conciliar os direitos ao respeito da vida privada e à proteção dos dados da pessoa em causa com a liberdade de informação dos internautas potencialmente interessados, o operador é obrigado, o mais tardar no momento em que o pedido de supressão das referências é apresentado, a organizar a lista de resultados de forma a que a imagem global que dela resulta para o Internauta reflita a situação judicial atual, o que obriga a que hiperligações para páginas web que contenham informações a este respeito surjam em primeiro lugar nessa lista (n.os 77 e 78).

Acórdão de 24 de setembro de 2019 (Grande Secção), Google (Alcance territorial da supressão de referências) (C-507/17, EU:C:2019:772) [70]

A Commission nationale de l'informatique et des libertés (Comissão Nacional da Informática e das Liberdades, CNIL, França) notificou a Google para que, quando aceitasse um pedido de supressão de referências, essa sociedade suprimisse da lista de resultados exibida, na sequência de uma pesquisa efetuada a partir do nome da pessoa em causa, as hiperligações que conduzem a páginas web que incluem dados pessoais relativos a essa pessoa em todas as extensões de nome de domínio do seu motor de busca. Uma vez que a Google recusou dar cumprimento a esta notificação, a CNIL aplicou-lhe uma sanção de 100 000 euros. O Conseil d'État, chamado a conhecer do processo pela Google, pediu que o Tribunal precisasse qual o alcance territorial da obrigação de um operador de um motor de busca de aplicar o direito à supressão de referências em aplicação da Diretiva 95/46.

O Tribunal começou por recordar a possibilidade de, com fundamento no direito da União, as pessoas singulares invocarem o seu direito à supressão de referências contra o operador de um motor de busca que dispõe de um ou mais estabelecimentos no território da União, independentemente do facto de o tratamento de dados pessoais (concretamente, a supressão de referências de hiperligações para páginas web nas quais figuram dados pessoais que dizem respeito à pessoa que invoca esse direito) ocorrer ou não na União [71].

No que respeita ao alcance do direito à supressão de referências, o Tribunal considerou que o operador de um motor de busca é obrigado a proceder à supressão de referências nas versões do seu motor que correspondam a todos os Estados-Membros e não em todas as versões do mesmo. Observou a este respeito que, embora uma supressão de referências fosse, tendo em conta as características da Internet e dos motores de busca, suscetível alcançar plenamente o objetivo do legislador da União, que consiste em garantir um nível elevado de proteção dos dados pessoais em toda a União, não resulta todavia de forma alguma do direito da União [72] que, para a realização desse objetivo, o legislador tenha optado por atribuir ao direito à

[70] Este acórdão foi apresentado no Relatório Anual de 2019, pp. 118 e 119.
[71] Artigo 4.°, n.° 1, alínea a), da Diretiva 95/46/CE, e artigo 3.°, n.° 1, do Regulamento 2016/679.
[72] Artigos 12.°, alínea b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46/CE, e artigo 17.°, n.° 1, do Regulamento 2016/679.

supressão de referências um alcance que ultrapasse o território dos Estados-Membros. Em particular, quando o direito da União institui mecanismos de cooperação entre autoridades de controlo dos Estados-Membros para alcançar uma decisão comum, baseada numa ponderação entre o direito à proteção da vida privada e dos dados pessoais, por um lado, e o interesse público dos diferentes Estados-Membros a aceder a uma informação, por outro, tais mecanismos não estão atualmente previstos no que respeita ao alcance de uma supressão de referências fora da União (n.os 62 e 73).

No estado atual do direito da União, incumbe ao operador do motor de busca proceder à supressão de referências pedida, não apenas na versão do motor correspondente ao Estado-Membro de residência do beneficiário dessa supressão de referências, mas também nas versões do motor que correspondem aos Estados-Membros, com vista, nomeadamente a assegurar um nível coerente e elevado de proteção em toda a União. Por outro lado, incumbe a esse operador tomar, se necessário, medidas suficientemente eficazes para impedir ou, pelo menos, desencorajar seriamente os internautas da União de acederem, eventualmente a partir de uma versão do motor de busca de um país terceiro, às hiperligações que são objeto de uma supressão de referências, incumbindo ao órgão jurisdicional nacional verificar se as medidas adotadas pelo operador cumprem esse requisito (n.° 70).

Por último, o Tribunal sublinhou que, embora o direito da União não obrigue o operador de um motor de busca a proceder a uma supressão de referências em todas as versões do seu motor, também não proíbe essa supressão. Por conseguinte, uma autoridade de controlo ou uma autoridade judiciária de um Estado-Membro continua a ser competente para proceder, à luz dos padrões nacionais de proteção dos direitos fundamentais, a uma ponderação entre o direito da pessoa em causa ao respeito da sua vida privada e à proteção dos seus dados pessoais, por um lado, e o direito à liberdade de informação, por outro, e, no final dessa ponderação, para, se for caso disso, intimar o operador desse motor de busca a proceder a uma supressão de referências em todas as versões do referido motor (n.os 65 e 72).

4. Consentimento do utilizador de um sítio Internet para o armazenamento de informações ou para o acesso a informações através de cookies

Acórdão de 1 de outubro de 2019 (Grande Secção), Planet49 (C-673/17, EU:C:2019:801) [73]

Com este acórdão, o Tribunal declarou que o consentimento para o armazenamento de informações ou para o acesso a informações através de *cookies* instalados no equipamento terminal do utilizador de um sítio Internet não é validamente dado quando a autorização resulta de uma opção pré-validada, e isso independentemente do facto de as informações em causa constituírem ou não dados pessoais. Além disso, o Tribunal precisou que o prestador de serviços deve indicar ao utilizador de um sítio Internet a duração do funcionamento dos *cookies* bem como a possibilidade ou não de terceiros terem acesso a esses *cookies*.

O litígio no processo principal tinha por objeto a organização de um jogo promocional pela Planet49 no sítio Internet www.dein-macbook.de. Para participarem nesse jogo, os internautas deviam comunicar o seu nome e a sua morada numa página web na qual se encontravam quadrículas de seleção. A quadrícula que autorizava a instalação dos *cookies* estava selecionada por defeito. Chamado a conhecer de um recurso interposto pela Federação alemã das organizações e associações de consumidores, o Bundesgerichtshof (Supremo Tribunal Federal, Alemanha) interrogou-se sobre a validade da obtenção do consentimento dos utilizadores através de uma opção pré-validada e a respeito do alcance da obrigação de informação que impende sobre o fornecedor do serviço.

O pedido de decisão prejudicial tinha essencialmente por objeto a interpretação do conceito de «consentimento» visado pela Diretiva 2002/58 [74], lido em conjugação com a Diretiva 95/46/CE [75], bem como com o RGPD [76].

Em primeiro lugar, o Tribunal observou que o artigo 2.°, alínea h), da Diretiva 95/46/CE, para o qual remete o artigo 2.°, alínea f), da Diretiva 2002/58, define consentimento como «qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento». Observou que a exigência de uma «manifestação» de vontade da pessoa em causa evoca claramente um comportamento ativo e não passivo. Ora, um consentimento dado através de uma opção pré-validada não implica um comportamento ativo por parte do utilizador de um sítio Internet. Além disso, a génese do artigo 5.°, n.° 3, da Diretiva 2002/58, que, desde a sua alteração pela Diretiva 2009/136, prevê que o utilizador deve ter «dado o seu consentimento» à colocação de *cookies*, tende a indicar que o consentimento do utilizador já não pode ser presumido e deve resultar de um comportamento ativo deste último. Por último, um consentimento ativo passou a estar previsto pelo RGPD [77], cujo artigo 4.°, n.° 11, exige uma manifestação de vontade que assuma

[73] Este acórdão foi apresentado no Relatório Anual de 2019, pp. 120 e 121.
[74] Artigos 2.°, alínea f), e 5.°, n.° 3, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO 2009, L 337, p. 11).
[75] Artigo 2.°, alínea h), da Diretiva 95/46/CE.
[76] Artigo 6.°, n.° 1, alínea a), do Regulamento 2016/679.
[77] *IDEM*.

nomeadamente a forma de um «ato positivo claro» e cujo considerando 32 exclui expressamente que haja consentimento em caso de «[s]ilêncio, [de] opções pré-validadas ou [de] omissão» (n.os 49, 52, 56 e 62).

O Tribunal declarou, por conseguinte, que o consentimento não é validamente dado quando o armazenamento de informações ou o acesso a informações já armazenadas no equipamento terminal do utilizador de um sítio Internet é autorizado através de uma opção pré-validada, que o utilizador deve desmarcar para recusar o seu consentimento. O Tribunal acrescentou que o facto de esse utilizador ativar o botão de participação no jogo promocional em causa não pode bastar para considerar que deu validamente o seu consentimento à colocação de cookies (n.º 63).

Em segundo lugar, o Tribunal de Justiça constatou que o artigo 5.º, n.º 3, da Diretiva 2002/58 visa proteger o utilizador contra qualquer ingerência na sua vida privada, independentemente da questão de saber se essa ingerência diz ou não respeito a dados pessoais. Daí decorre que o conceito de «consentimento» não deve ser interpretado de forma diferente consoante as informações armazenadas ou consultadas no equipamento terminal do utilizador de um sítio Internet constituam ou não dados pessoais (n.os 69 e 71).

Em terceiro lugar, o Tribunal salientou que o artigo 5.º, n.º 3, da Diretiva 2002/58 exige que o utilizador tenha dado o seu acordo, depois de ter recebido informações claras e completas, nomeadamente a respeito da finalidade do tratamento. Ora, uma informação clara e completa deve permitir ao utilizador determinar facilmente as consequências do consentimento que poderia dar e garantir que esse consentimento seja dado com pleno conhecimento de causa. A este respeito, o Tribunal considerou que a duração de funcionamento dos *cookies,* bem como a possibilidade de esses terceiros terem ou não acesso a tais cookies, fazem parte da informação clara e completa que deve ser dada ao utilizador de um sítio Internet pelo fornecedor de serviços (n.os 73 a 75 e 81).

VI. Autoridades nacionais de controlo

1. Alcance da exigência de independência

Acórdão de 9 de março de 2010 (Grande Secção), Comissão/Alemanha (C-518/07, EU:C:2010:125) [78]

Na sua petição, a Comissão pedia ao Tribunal de Justiça que declarasse que a República Federal da Alemanha, ao submeter à tutela do Estado as autoridades de controlo competentes para fiscalizar o tratamento de dados pessoais no setor não público nos diferentes *Länder*, transpondo, assim, de forma errada a exigência de «total independência» das autoridades encarregadas de garantir a proteção desses dados, não cumpriu as obrigações que lhe incumbem por força do artigo 28.º, n.º 1, segundo parágrafo, da Diretiva 95/46.

[78] Este acórdão foi apresentado no Relatório Anual de 2010, p. 34.

A República Federal da Alemanha, por seu turno, considerava que o artigo 28.°, n.° 1, segundo parágrafo, da Diretiva 95/46 exige uma independência funcional das autoridades de controlo, no sentido de que essas autoridades devem ser independentes do setor não público sujeito à sua fiscalização e não devem estar expostas a influências externas. Ora, na sua opinião, a tutela do Estado exercida nos *Landër* alemães não constituía uma tal influência externa, tratando-se antes de um mecanismo de vigilância interna da Administração, instituído por autoridades que fazem parte do mesmo aparelho administrativo que as autoridades de controlo e que estão obrigadas, como estas autoridades, a cumprir os objetivos da Diretiva 95/46.

O Tribunal declarou que a garantia de independência das autoridades nacionais de controlo prevista na Diretiva 95/46 visa assegurar a eficácia e a fiabilidade da fiscalização do respeito das disposições em matéria de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e deve ser interpretada à luz deste objetivo. Não foi estabelecida para conferir um estatuto especial às próprias autoridades e aos seus agentes, mas com vista a reforçar a proteção das pessoas e dos organismos abrangidos pelas suas decisões, sendo que as autoridades de supervisão devem, portanto, no exercício das suas funções, agir de forma objetiva e imparcial (n.° 25).

O Tribunal considerou que essas autoridades de controlo competentes para fiscalizar o tratamento dos dados pessoais no setor não público devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. Essa independência exclui não só qualquer influência exercida pelos organismos de fiscalização mas também qualquer instrução ou qualquer outra influência externa, direta ou indireta, que possam pôr em causa o cumprimento, pelas referidas autoridades, da sua tarefa de estabelecer um justo equilíbrio entre a proteção do direito à vida privada e a livre circulação de dados pessoais. O mero risco de as autoridades de tutela poderem exercer uma influência política nas decisões das autoridades de controlo é suficiente para impedir o exercício independente das suas funções. Por um lado, daí poderia resultar uma «obediência antecipada» dessas autoridades atendendo à prática decisória da autoridade de tutela. Por outro lado, o papel de guardiãs do direito à vida privada que as referidas autoridades de controlo desempenham exige que as suas decisões e, consequentemente, elas próprias, estejam acima de qualquer suspeita de parcialidade. Segundo o Tribunal, a tutela do Estado exercida sobre as autoridades nacionais de controlo não é, por conseguinte, compatível com a exigência de independência (n.os 30, 36, 37 e disp.).

Acórdão de 16 de outubro de 2012 (Grande Secção) Comissão/Áustria (C-614/10, EU:C:2012:631)

Na sua petição, a Comissão pediu ao Tribunal de Justiça que declarasse que, ao não adotar todas as disposições necessárias para que a legislação em vigor na Áustria cumprisse o critério de independência no que respeita à Datenschutzkommission (Comissão para a proteção dos dados), instituída como autoridade de controlo da proteção de dados pessoais, a Áustria não cumpriu as obrigações que lhe incumbem por força do artigo 28.°, n.° 1, segundo parágrafo, da Diretiva 95/46.

O Tribunal constatou um incumprimento por parte da Áustria, considerando, em substância, que não cumpre o critério de independência da autoridade de controlo, estabelecido pela Diretiva 95/46, o Estado-Membro que institui um quadro regulamentar ao abrigo do qual o membro administrador da referida autoridade é um funcionário do Estado, sujeito a supervisão,

cujo gabinete está integrado nos serviços do governo nacional, e relativamente à qual o chefe do governo nacional dispõe de um direito incondicional à informação sobre todos os aspetos da sua gestão (n.° 66 e disp).

O Tribunal recordou, antes de mais, que a expressão «com total independência» constante do artigo 28.°, n.° 1, segundo parágrafo, da Diretiva 95/46, implicam que as autoridades de controlo devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. Neste aspeto, o facto de essa autoridade beneficiar de uma independência funcional na medida em que os seus membros são independentes e não estão vinculados por nenhuma instrução no exercício da sua função não basta, por si só, para preservar a autoridade de controlo de qualquer influência externa. Ora, a independência exigida neste contexto visa excluir não só a influência direta, sob a forma de instruções, mas também qualquer forma de influência indireta suscetível de orientar as decisões da autoridade de controlo. Por outro lado, o papel de guardiãs do direito à vida privada que as referidas autoridades desempenham exige que as suas decisões e, consequentemente, elas próprias, estejam acima de qualquer suspeita de parcialidade (n.os 41 a 43 e 52).

O Tribunal precisou que, para poder cumprir o critério de independência enunciado na referida disposição da Diretiva 95/46, uma autoridade nacional de controlo não deve dispor de uma rubrica orçamental autónoma, à semelhança da prevista no artigo 43.°, n.° 3, do Regulamento - n.° 45/2001. Com efeito, os Estados-Membros não são obrigados a reproduzir, na sua legislação nacional, disposições análogas às do capítulo V do Regulamento n.° 45/2001 para garantir uma independência total à(s) sua(s) autoridade(s) de controlo, pelo que podem prever que, do ponto de vista orçamental, a autoridade de controlo depende de um determinado departamento ministerial. Contudo, a atribuição dos meios humanos e materiais necessários a essa autoridade não deve impedi-la de exercer as suas funções «com total independência» na aceção do artigo 28.°, n.° 1, segundo parágrafo, da Diretiva 95/46 (n.° 58).

Acórdão de 8 de abril de 2014 (Grande Secção), Comissão/Hungria (C-288/12, EU:C:2014:237) [79]

Neste processo, a Comissão pedia ao Tribunal que declarasse que, ao fazer cessar antecipadamente o mandato da autoridade de controlo da proteção de dados pessoais, a Hungria não cumpriu as obrigações que lhe incumbem por força da Diretiva 95/46.

O Tribunal declarou que um Estado-Membro que faz cessar antecipadamente o mandato da autoridade de controlo da proteção de dados pessoais não cumpre as obrigações que lhe incumbem por força da Diretiva 95/46/CE (n.° 62 e disp. 1).

Com efeito, segundo o Tribunal, a independência de que devem gozar as autoridades de controlo competentes para a supervisão do tratamento dos referidos dados exclui, designadamente, qualquer instrução e qualquer outra influência externa, sob qualquer forma, seja direta ou indireta, suscetíveis de orientar as suas decisões e que podem assim pôr em causa o cumprimento, pelas referidas autoridades, da sua função de estabelecer um justo equilíbrio entre a proteção da vida privada e a livre circulação dos dados de natureza pessoal (n.° 51).

[79] Este acórdão foi apresentado no Relatório Anual de 2014, p. 62.

Além disso, o Tribunal recordou que, na medida em que a independência funcional não basta, por si só, para resguardar as autoridades de controlo de qualquer influência externa, o mero risco de as autoridades de tutela de um Estado poderem exercer uma influência política nas decisões das autoridades de controlo é suficiente para impedir o exercício independente das funções destas. Ora, se cada Estado-Membro pudesse fazer cessar o mandato de uma autoridade de controlo antes do termo inicialmente previsto, sem respeitar as regras e garantias previamente estabelecidas para esse efeito pela legislação aplicável, a ameaça dessa cessação antecipada que pairaria sobre essa autoridade ao longo do exercício do seu mandato poderia levar a uma forma de obediência desta ao poder político, incompatível com a referida exigência de independência. Além disso, nessa situação, não se pode considerar que a autoridade de controlo pode, em qualquer circunstância, operar acima de qualquer suspeita de parcialidade (n.os 52 a 55).

2. Determinação do direito aplicável e da autoridade de controlo competente

Acórdão de 1 de outubro de 2015, Weltimmo (C-230/14, EU:C:2015:639) [80]

A Nemzeti Adatvédelmi és Információszabadság Hatóság (Autoridade nacional para a proteção dos dados e a liberdade de informação, Hungria) aplicou uma coima à Weltimmo, sociedade registada na Eslováquia, que explorava sítios Internet de anúncios imobiliários de bens situados na Hungria, pelo facto de esta não ter apagado os dados pessoais dos anunciantes desses sítios, apesar do pedido destes nesse sentido, e pelo facto de aquela sociedade ter comunicado esses dados a agências de recuperação de crédito com vista a obter o pagamento de faturas não pagas. Segundo a autoridade de controlo húngara, a empresa Weltimmo tinha, desse modo, violado a legislação húngara que transpõe a Diretiva 95/46.

Chamada a conhecer de um recurso, a Kúria (Supremo Tribunal, Hungria) teve dúvidas quanto à determinação do direito aplicável e dos poderes de que dispõe a autoridade de controlo húngara com base nos artigos 4.°, n.° 1, e artigo 28.° da Diretiva 95/46. Por conseguinte, submeteu várias questões prejudiciais ao Tribunal.

No que respeita ao direito nacional aplicável, o Tribunal declarou que o artigo 4.°, n.° 1, alínea a), da Diretiva 95/46 permite a aplicação da legislação relativa à proteção de dados pessoais de um Estado-Membro diferente daquele em que o responsável pelo tratamento desses dados está registado, desde que este exerça, através de uma instalação estável no território desse Estado-Membro, uma atividade efetiva e real, ainda que mínima, em cujo contexto esse tratamento é efetuado. Para determinar se é esse o caso, o órgão jurisdicional de reenvio pode, designadamente, ter em conta, por um lado, que a atividade do responsável pelo referido tratamento, no âmbito da qual este último tenha lugar, consiste na exploração de sítios Internet de anúncios de imobiliários de bens situados no território desse Estado-Membro e que tenham sido redigidos na língua deste e que, por conseguinte, é principalmente, ou mesmo totalmente, direcionada para esse Estado-Membro. Por outro lado, o órgão jurisdicional de reenvio também pode ter em conta o facto de esse responsável dispor de um representante no referido Estado-Membro, encarregado de cobrar os créditos resultantes dessa atividade e de representá-lo em processos administrativos e judiciais relativos ao tratamento dos dados em

[80] Este acórdão foi apresentado no Relatório Anual de 2015, p. 55.

causa. Em contrapartida, o Tribunal considerou que a questão da nacionalidade das pessoas afetadas por esse tratamento de dados é desprovida de pertinência (n.° 41 e disp. 1).

No que respeita à competência e aos poderes da autoridade de controlo à qual tenham sido apresentadas queixas, em conformidade com o artigo 28.°, n.° 4, da Diretiva 95/46, o Tribunal considerou que esta autoridade pode analisar essas queixas independentemente do direito aplicável e inclusivamente antes de saber qual é o direito nacional aplicável ao tratamento em causa (n.° 54). No entanto, se concluir que é aplicável o direito de outro Estado-Membro, não poderá aplicar sanções fora do território do Estado-Membro a que pertence. Nessa situação, cabe-lhe, em aplicação do dever de cooperação previsto no artigo 28.°, n.° 6, da mesma diretiva, pedir à autoridade de controlo desse outro Estado-Membro que verifique a existência de uma eventual infração a esse direito e que aplique sanções se este último o permitir, baseando-se, se for caso disso, nas informações que lhe tiver transmitido (n.os 57, 60 e disp. 2).

3. Poderes das autoridades nacionais de controlo

Acórdão de 6 de outubro de 2015 (Grande Secção) Schrems (C-362/14, EU:C:2015:650)

Neste processo (ver também a rubrica IV, intitulada «Transferência de dados pessoais para países terceiros»), o Tribunal declarou nomeadamente que as autoridades nacionais de controlo são competentes para controlar as transferências de dados pessoais para países terceiros.

A este respeito, o Tribunal começou por constatar que as autoridades nacionais de controlo dispõem de um amplo leque de poderes, enumerados de forma não exaustiva no artigo 28.°, n.° 3, da Diretiva 95/46, que constituem os meios necessários para o desempenho das suas funções. Assim, as referidas autoridades gozam, nomeadamente, de poderes de inquérito, tais como recolher todas as informações necessárias ao desempenho das suas funções de controlo, de poderes efetivos de intervenção, tais como proibir temporária ou definitivamente um tratamento de dados ou ainda do poder de intervir em processos judiciais (n.° 43).

No que diz respeito ao poder de controlar as transferências de dados pessoais para os países terceiros, o Tribunal declarou que é certo que decorre do artigo 28.°, n.os 1 e 6, da Diretiva 95/46 que os poderes das autoridades nacionais de controlo respeitam aos tratamentos de dados pessoais efetuados no território do Estado-Membro dessas autoridades, pelo que não dispõem de poderes, ao abrigo deste artigo 28.°, relativamente aos tratamentos de tais dados efetuados no território de um país terceiro (n.° 44).

No entanto, a operação que consiste em transferir dados pessoais a partir de um Estado-Membro para um país terceiro constitui, enquanto tal, um tratamento de dados pessoais efetuado no território de um Estado-Membro. Por conseguinte, uma vez que as autoridades nacionais de controlo estão encarregadas, em conformidade com o artigo 8.°, n.° 3, da Carta e com o artigo 28.° da Diretiva 95/46, do controlo do cumprimento das regras da União relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, cada uma delas tem competência para verificar se uma transferência de dados pessoais do Estado-Membro dessa autoridade para um país terceiro respeita as exigências estabelecidos por esta diretiva (n.os 45 e 47).

Acórdão de 5 de junho de 2018 (Grande Secção), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

Neste acórdão (ver igualmente a rubrica II.5., intitulada «Conceito de 'responsável pelo tratamento de dados pessoais'»), relativo, nomeadamente, à interpretação dos artigos 4.° e 28.° da Diretiva 95/46, o Tribunal pronunciou-se a respeito do alcance dos poderes de intervenção de que as autoridades de controlo dispõem num contexto de tratamento de dados pessoais que implica a participação de vários atores.

Assim, o Tribunal declarou que, quando uma empresa estabelecida fora da União Europeia (como a sociedade americana Facebook) dispõe de vários estabelecimentos em diferentes Estados-Membros, a autoridade de controlo de um Estado-Membro pode exercer os poderes que o artigo 28.°, n.° 3, desta diretiva lhe confere relativamente a um estabelecimento desta empresa situado no território desse Estado-Membro (concretamente a Facebook Germany), ainda que, em resultado da distribuição interna das funções do grupo, por um lado, este estabelecimento só seja responsável pela venda de espaços publicitários e por outras atividades de marketing no território do referido Estado-Membro e, por outro, a responsabilidade exclusiva pela recolha e pelo tratamento dos dados pessoais incumba, para todo o território da União, a um estabelecimento situado noutro Estado-Membro (concretamente a Facebook Ireland) (n.° 64 e disp. 2).

Além disso, o Tribunal precisou que, quando a autoridade de controlo de um Estado-Membro pretende exercer, em relação a um organismo estabelecido no território desse Estado-Membro, os poderes de intervenção referidos no artigo 28.°, n.° 3, da Diretiva 95/46 devido a violações às regras em matéria de proteção de dados pessoais, cometidas por um terceiro responsável pelo tratamento desses dados e que tem sede noutro Estado-Membro (concretamente, a Facebook Ireland), esta autoridade de controlo é competente para apreciar, de maneira autónoma em relação à autoridade de controlo deste último Estado-Membro (Irlanda), a legalidade desse tratamento de dados e pode exercer os seus poderes de intervenção em relação ao organismo estabelecido no seu território sem ter de solicitar previamente a intervenção da autoridade de controlo do outro Estado-Membro (n.° 74 e disp. 3).

Acórdão de 15 de junho de 2021 (Grande Secção), Facebook Ireland e o. (C-645/19, EU:C:2021:483)

Em 11 de setembro de 2015, o presidente da Comissão de Proteção da Vida Privada belga (a seguir «CPVP») intentou no Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunal de Primeira Instância de língua neerlandesa de Bruxelas, Bélgica), uma ação inibitória contra a Facebook Ireland, a Facebook Inc. e a Facebook Belgium, na qual pedia que fosse posto termo a violações, pretensamente cometidas pela Facebook, da legislação relativa à proteção de dados. Estas violações consistiam nomeadamente na recolha e na utilização de informações sobre o comportamento de navegação dos internautas belgas, detentores ou não de uma conta Facebook, através de diferentes tecnologias, como *cookies*, módulos sociais [81] ou *pixels*.

Em 16 de fevereiro de 2018, o referido tribunal declarou-se competente para conhecer desta ação inibitória e, quanto ao mérito, declarou que a rede social Facebook não tinha informado os

[81] Por exemplo, os botões «Gosto» ou «Partilhar».

internautas belgas de forma suficiente sobre a recolha e a utilização das informações em causa. Por outro lado, o consentimento dado pelos internautas para a recolha e para o tratamento das referidas informações foi julgado inválido.

Em 2 de março de 2018, a Facebook Ireland, a Facebook Inc. e a Facebook Belgium interpuseram recurso daquela decisão para o hof van beroep te Brussel (Tribunal de Recurso de Bruxelas), órgão jurisdicional de reenvio no presente processo. Naquele órgão jurisdicional, a Autoridade de Proteção de Dados (Bélgica) (APD) atuou como sucessora legal do presidente da CPVP. O órgão jurisdicional de reenvio só se declarou competente para se pronunciar sobre o recurso interposto pela Facebook Belgium.

O órgão jurisdicional de reenvio manifestou dúvidas a respeito do impacto da aplicação do mecanismo de «balcão único» previsto no RGPD [82] nas competências da APD e questionou-se, mais especificamente, sobre a questão de saber se, em relação aos factos posteriores à entrada em vigor do RGPD, a saber em 25 de maio de 2018, a APD pode agir judicialmente contra a Facebook Belgium, uma vez que foi a Facebook Ireland que foi identificada como responsável pelo tratamento dos dados em causa. Com efeito, desde essa data, nomeadamente em aplicação do princípio do «balcão único» previsto no RGPD, só o Comissário para a Proteção de Dados irlandês é competente para intentar uma ação inibitória, sob o controlo dos órgãos jurisdicionais irlandeses (n.os 36 e 37).

No seu acórdão, proferido em formação de Grande Secção, o Tribunal de Justiça precisa os poderes das autoridades nacionais de controlo no âmbito do RGPD. Assim, declara nomeadamente que este regulamento autoriza, em certas condições, que uma autoridade de controlo de um Estado-Membro exerça o seu poder de dar conhecimento de quaisquer pretensas violações ao RGPD às autoridades judiciais deste Estado-Membro e intente ou de outro modo intervenha em processos judiciais relativos a um tratamento de dados transfronteiriço [83], embora não seja a autoridade de controlo principal responsável por esse tratamento (disp. 1).

Em primeiro lugar, o Tribunal precisa as condições nas quais uma autoridade nacional de controlo, que não tem a qualidade de autoridade de controlo principal no que respeita a um tratamento transfronteiriço, deve exercer o seu poder de dar conhecimento de quaisquer pretensas violações do RGPD às autoridades judiciais de um Estado-Membro e, se necessário, intentar ações ou de outro modo intervir em processos judiciais para assegurar a aplicação deste regulamento. Assim, por um lado, o RGPD deve conferir a esta autoridade de controlo competência para adotar uma decisão que constate que este tratamento viola as regras previstas neste regulamento e, por outro, este poder deve ser exercido respeitando os procedimentos de cooperação e de controlo da coerência previstos neste regulamento [84] (n.º 75 e disp. 1).

Com efeito, no que respeita aos tratamentos transfronteiriços, o RGPD prevê o mecanismo do «balcão único» [85], que se baseia numa repartição das competências entre uma «autoridade de

82 Nos termos do artigo 56.º, n.º 1, do RGPD: «Sem prejuízo do disposto no artigo 55.º, a autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante é competente para agir como autoridade de controlo principal para o tratamento transfronteiriço efetuado pelo referido responsável pelo tratamento ou subcontratante.»

83 Na aceção do artigo 4.º, ponto 23, do RGPD.

84 Previstos nos artigos 56.º e 60.º do RGPD.

85 Artigo 56.º, n.º 1, do RGPD.

controlo principal» e as outras autoridades nacionais de controlo interessadas. Este mecanismo exige uma cooperação estreita, leal e eficaz entre estas autoridades, para assegurar uma proteção coerente e homogénea das regras relativas à proteção dos dados pessoais e assim preservar o seu efeito útil. O RGPD consagra, a este respeito, a competência de princípio da autoridade de controlo principal para adotar uma decisão que constate que um tratamento transfronteiriço viola as regras previstas neste regulamento [86], ao passo que a competência das outras autoridades nacionais de controlo para adotarem tal decisão, ainda que a título provisório, constitui a exceção [87]. No entanto, ao exercer as suas competências, a autoridade de controlo principal não pode prescindir de um diálogo indispensável nem de uma cooperação leal e eficaz com as outras autoridades de controlo interessadas. Deste modo, no âmbito desta cooperação, a autoridade de controlo principal não pode ignorar os pontos de vista das outras autoridades de controlo interessadas e qualquer objeção pertinente e fundamentada formulada por uma destas últimas autoridades tem por efeito bloquear, pelo menos temporariamente, a adoção do projeto de decisão da autoridade de controlo principal (n.os 50 a 53, 56 a 59 e 63 a 65).

O Tribunal precisa que a circunstância de uma autoridade de controlo de um Estado-Membro, diferente da autoridade de controlo principal, relativamente a um tratamento de dados transfronteiriço só poder exercer o poder de dar conhecimento de quaisquer pretensas violações cometidas ao RGPD às autoridades jurisdicionais deste Estado e de intentar ações ou de outro modo intervir em processos judiciais respeitando as regras de repartição das competências decisórias entre a autoridade de controlo principal e as outras autoridades de controlo [88] é conforme com os artigos 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais da União Europeia, que garantem à pessoa em causa, respetivamente, o direito à proteção dos dados de caráter pessoal que lhe digam respeito e o direito à ação (n.° 67).

Em segundo lugar, o Tribunal declara que, em caso de tratamento de dados transfronteiriço, o exercício do poder de uma autoridade de controlo de um Estado-Membro, diferente da autoridade de controlo principal, para intentar uma ação judicial [89] não exige que o responsável pelo tratamento ou o subcontratante para o tratamento transfronteiriço de dados pessoais contra o qual esta ação é intentada disponha de um estabelecimento principal ou de outro estabelecimento no território desse Estado-Membro. No entanto, o exercício deste poder deve ser abrangido pelo âmbito de aplicação territorial do RGPD [90], o que pressupõe que o responsável pelo tratamento ou o subcontratante para o tratamento transfronteiriço disponha de um estabelecimento no território da União (n.os 80, 83, 84 e disp. 2).

Em terceiro lugar, o Tribunal declara que, em caso de tratamento de dados transfronteiriço, o poder de uma autoridade de controlo de um Estado-Membro, diferente da autoridade de controlo principal, de dar conhecimento de quaisquer pretensas violações ao RGPD a uma autoridade judicial deste Estado e, se necessário, de intentar ações ou de outro modo intervir em processos judiciais, pode ser exercido tanto em relação ao estabelecimento principal do

---

86 Artigo 60.°, n.° 7, do RGPD.

87 O artigo 56.°, n.° 2, e o artigo 66.° do RGPD consagram as exceções ao princípio da competência decisória da autoridade de controlo principal.

88 Previstas nos artigos 55.° e 56.°, lidos em conjunto com o artigo 60.° do RGPD.

89 Nos termos do artigo 58.°, n.° 5, do RGPD.

90 O artigo 3.°, n.° 1, do RGPD prevê que este regulamento se aplica ao tratamento dos dados pessoais efetuado «no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União».

responsável pelo tratamento que se encontre no Estado-Membro a que pertence esta autoridade como em relação a outro estabelecimento deste responsável, desde que a ação judicial diga respeito a um tratamento de dados efetuado no âmbito das atividades deste estabelecimento e que a referida autoridade seja competente para exercer esse poder.

No entanto, o Tribunal precisa que o exercício deste poder pressupõe que o RGPD seja aplicável. No presente caso, estando as atividades do estabelecimento do grupo Facebook situado na Bélgica indissociavelmente ligadas ao tratamento dos dados pessoais em causa no processo principal, pelo qual a Facebook Ireland é responsável no que respeita ao território da União, este tratamento é efetuado «no contexto das atividades de um estabelecimento de um responsável pelo tratamento» e é por conseguinte efetivamente abrangido pelo âmbito de aplicação do RGPD (n.os 94 a 96 e disp. 3).

Em quarto lugar, o Tribunal declara que, quando uma autoridade de controlo de um Estado-Membro diferente da «autoridade de controlo principal» tiver intentado, antes da data de entrada em vigor do RGPD, uma ação judicial relativa a um tratamento transfronteiriço de dados pessoais, essa ação pode manter-se, ao abrigo do direito da União, com fundamento nas disposições da Diretiva 95/46 a qual continua a ser aplicável no que respeita às infrações às regras nela previstas que tenham sido cometidas até à data em que esta diretiva foi revogada. Além disso, esta ação pode ser intentada por esta autoridade a título de infrações cometidas após a data de entrada em vigor do RGPD, desde que tal suceda ao abrigo de uma das situações nas quais, a título de exceção, este regulamento confere a esta mesma autoridade competência para adotar uma decisão que constate que o tratamento de dados em questão viola as regras previstas neste regulamento e desde que sejam respeitados os procedimentos de cooperação e de controlo da coerência previstos neste último (n.° 105 e disp. 4).

Em quinto lugar e último lugar, o Tribunal reconhece o efeito direto da disposição do RGPD ao abrigo da qual cada Estado-Membro prevê, por lei, que a sua autoridade de controlo tem poder para dar conhecimento de quaisquer violações deste regulamento às autoridades judiciais e, se necessário, intentar ações ou de outro modo intervir em processos judiciais. Por conseguinte, tal autoridade pode invocar esta disposição para instaurar ou dar continuidade a uma ação judicial contra particulares, ainda que esta disposição não tenha sido especificamente implementada na legislação do Estado-Membro em causa (n.° 113 e disp. 5).

VII. Aplicação territorial da legislação europeia

Acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, EU:C:2014:317)

Neste acórdão (ver também a rubrica II.3, intitulada «Conceito de 'tratamento de dados pessoais'», e V.1, intitulada «Direito de oposição ao tratamento dos dados pessoais ('direito a ser esquecido')»), o Tribunal também se pronunciou sobre o âmbito de aplicação geográfico da Diretiva 95/46.

Assim, o Tribunal declarou que é efetuado um tratamento de dados pessoais no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um

Estado-Membro, na aceção da Diretiva 95/46, quando o operador de um motor de busca, ainda que tenha a sua sede num Estado terceiro, cria num Estado-Membro uma sucursal ou uma filial destinada a assegurar a promoção e a venda dos espaços publicitários propostos por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro (n.os 55, 60 e disp. 2).

Com efeito, nestas circunstâncias, as atividades do operador do motor de busca e as do seu estabelecimento situado num Estado-Membro, embora distintas, estão indissociavelmente ligadas, uma vez que as atividades relativas aos espaços publicitários constituem o meio para tornar o motor de busca em causa economicamente rentável e que esse motor é, ao mesmo tempo, o meio que permite realizar essas atividades (n.° 56).

VIII. Direito de acesso do público aos documentos das instituições da União Europeia e proteção dos dados pessoais

Acórdão de 29 de junho de 2010 (Grande Secção), Comissão/Bavarian Lager (C-28/08 P, EU:C:2010:378)

A Bavarian Lager, sociedade criada para importar cerveja alemã para venda em estabelecimentos de bebidas no Reino Unido, não pôde vender o seu produto, uma vez que um grande número de empresários de estabelecimentos de venda de bebidas do Reino Unido estavam vinculados por contratos de compra exclusiva que os obrigavam a abastecer-se de cerveja junto de certos fabricantes de cerveja.

Por força da regulamentação do Reino Unido relativa ao fornecimento de cerveja (a seguir «GBP»), os fabricantes de cerveja britânicos eram obrigados a conceder aos gerentes dos pubs a possibilidade de comprarem uma cerveja proveniente de outra fábrica, na condição de ser acondicionada em barril. Ora, a maior parte das cervejas produzidas fora do Reino Unido não podiam ser consideradas «cervejas vendidas em barril», na aceção da GBP, e, por conseguinte, não se enquadravam no seu âmbito de aplicação. Considerando que a referida regulamentação constituía uma medida de efeito equivalente a uma restrição quantitativa às importações, a Bavarian Lager apresentou uma denúncia à Comissão.

Durante o processo por incumprimento iniciado pela Comissão contra o Reino Unido, os representantes das administrações comunitária e britânica, bem como representantes da Confederação dos fabricantes de cerveja do mercado comum (CBMC), participaram numa reunião que decorreu em 11 de outubro de 1996. Depois de ter sido informada pelas autoridades inglesas da alteração da regulamentação em causa no sentido de permitir a venda de cerveja engarrafada como cerveja de proveniência diferente, como a cerveja em barril, a Comissão informou a Bavarian Lager da suspensão do processo por incumprimento.

A Bavarian Lager apresentou um pedido com vista a obter a ata completa da reunião de outubro de 1996, com a menção do nome de todos os participantes, o qual foi indeferido pela Comissão por decisão de 18 de março de 2004, com fundamento, nomeadamente, na proteção da vida privada, como garantida pelo Regulamento n.° 45/2001.

A Bavarian Lager interpôs um recurso no Tribunal Geral no qual pedia a anulação desta decisão da Comissão. Por acórdão de 8 de novembro de 2007, o Tribunal Geral anulou a decisão da Comissão, considerando, nomeadamente, que a simples inscrição do nome dos interessados na lista das pessoas que participaram numa reunião em nome da entidade que representavam não lesava os interesses nem comprometia a vida privada dessas pessoas. A Comissão, apoiada pelo Reino Unido e pelo Conselho, interpôs no Tribunal de Justiça um recurso deste acórdão do Tribunal Geral.

O Tribunal de Justiça começou por observar que, quando um pedido baseado no Regulamento n.º 1049/2001 [91], relativo ao acesso aos documentos, se destina a obter o acesso a documentos que incluem dados pessoais, as disposições do Regulamento n.º 45/2001 passam a ser integralmente aplicáveis, incluindo a disposição que impõe ao destinatário da transferência de dados pessoais a obrigação de demonstrar a necessidade da sua divulgação e a disposição que confere à pessoa em causa a possibilidade de se opor em qualquer momento, por razões imperiosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de um tratamento (n.º 63).

Em seguida, o Tribunal de Justiça declarou que a lista dos participantes numa reunião realizada no âmbito de um processo por incumprimento que figuram na ata da referida reunião continha dados pessoais, na aceção do artigo 2.º, alínea a), do Regulamento (CE) n.º 45/2001, uma vez que as pessoas que participaram nesta reunião podiam ser identificadas (n.º 70).

Por último, concluiu que, ao exigir que, relativamente às pessoas que não deram o seu consentimento expresso à divulgação dos dados pessoais que lhes diziam respeito contidas neste relatório, a necessidade da transferência desses dados pessoais fosse demonstrada, a Comissão tinha dado cumprimento às disposições do artigo 8.º, alínea b), do referido regulamento (n.º 77).

Com efeito, quando, no âmbito de um pedido de acesso à referida ata ao abrigo do Regulamento n.º 1049/2001, não é fornecida nenhuma justificação expressa e legítima nem nenhum argumento convincente para demonstrar a necessidade da transferência desses dados pessoais, a Comissão não pode ponderar os diferentes interesses das partes em causa. A comissão também não podia verificar se não existiam motivos para supor que os interesses legítimos das pessoas em causa podiam ser lesados, como prevê o artigo 8.º, alínea b), do Regulamento n.º 45/2001 (n.º 78) [92].

Acórdão de 16 de julho de 2015, ClientEarth e PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

A Autoridade Europeia para a Segurança dos Alimentos (EFSA) constituiu um grupo de trabalho a fim de elaborar uma orientação para indicar a maneira de aplicar o artigo 8.º, n.º 5, do Regulamento (CE) n.º 1107/2009 [93], nos termos do qual o autor de um pedido de autorização de colocação no mercado de um produto fitofarmacêutico deve juntar ao processo a literatura científica existente, como determinada pela EFSA, validada pela comunidade científica, sobre os

[91] Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO 2001, L 145, p. 43).

[92] Este acórdão foi apresentado no Relatório Anual de 2010, p. 14.

[93] Regulamento (CE) n.º 1107/2009 do Parlamento Europeu e do Conselho, de 21 de outubro de 2009, relativo à colocação dos produtos fitofarmacêuticos no mercado e que revoga as Diretivas 79/117/CEE e 91/414/CEE do Conselho (JO 2009, L 309, p. 1).

efeitos secundários da substância ativa e dos seus metabolitos relevantes na saúde, no ambiente e nas espécies não visadas.

O projeto de orientação foi submetido a consulta pública, tendo a ClientEarth e a Pesticide Action Network Europe (PAN Europe) apresentado observações sobre o projeto. Neste contexto, apresentaram conjuntamente à EFSA um pedido de acesso a documentos relativos à preparação do projeto de orientação, incluindo as observações dos peritos externos.

A EFSA autorizou a ClientEarth e a PAN Europe a acederem, nomeadamente, às observações individuais dos peritos externos relativas ao projeto de orientação. Indicou, porém, que tinha ocultado o nome desses peritos, de acordo com o artigo 4.°, n.° 1, alínea b), do Regulamento n.° 1049/2001 e com a legislação da União sobre proteção de dados pessoais, nomeadamente o Regulamento n.° 45/2001. Alegou, a esse respeito, que a divulgação do nome desses peritos correspondia a uma transferência de dados pessoais, na aceção do artigo 8.° do Regulamento n.° 45/2001, e que neste caso não estavam preenchidas as condições para essa transferência previstas no referido artigo.

Por conseguinte, a ClientEarth e a PAN Europe interpuseram recurso de anulação da referida decisão da EFSA no Tribunal Geral. O Tribunal Geral negou provimento ao recurso, tendo a ClientEarth e a PAN Europe interposto recurso do acórdão [94] do Tribunal Geral para o Tribunal de Justiça.

Em primeiro lugar, o Tribunal de Justiça salientou que, atendendo a que a informação pedida permitia relacionar um determinado perito com uma dada observação, a mesma dizia respeito a pessoas singulares identificadas e, portanto, constituía um conjunto de dados pessoais, na aceção do artigo 2.°, alínea a), do Regulamento n.° 45/2001. Dado que os conceitos de «dados pessoais», na aceção do artigo 2.°, alínea a), do Regulamento n.° 45/2001 e de «dados relativos à vida privada» não se confundem, o Tribunal de Justiça considerou, além disso, que a alegação da ClientEarth e da PAN Europe de que a informação em causa não estava abrangida pelo âmbito da vida privada desses peritos, era inoperante (n.os 29 e 32).

O Tribunal de Justiça analisou em segundo lugar o argumento da ClientEarth e da PAN Europe baseado na existência de um clima de desconfiança em relação à EFSA, frequentemente acusada de parcialidade por recorrer a peritos com interesses pessoais ditados pelas suas ligações aos meios industriais, e na necessidade de garantir a transparência do processo decisório dessa autoridade. Este argumento baseava-se num estudo que fazia referências a ligações da maioria dos peritos que eram membros de um grupo de trabalho da EFSA com organizações lobistas no domínio da indústria. A esse respeito, o Tribunal de Justiça declarou que a obtenção da informação controvertida era necessária para proceder à verificação concreta da imparcialidade de cada um desses peritos no desempenho da sua missão científica ao serviço da EFSA. Consequentemente, o Tribunal de Justiça anulou o acórdão do Tribunal Geral, declarando que foi erradamente que o Tribunal Geral considerou que este argumento da ClientEarth e da PAN Europe não bastava para demonstrar a necessidade da transferência da informação controvertida (n.os 57 a 59).

[94] Acórdão do Tribunal Geral de 13 de setembro de 2013, ClientEarth e PAN Europe/EFSA (T-214/11, EU:T:2013:483).

Em terceiro lugar, para apreciar a legalidade da decisão controvertida da EFSA, o Tribunal de Justiça examinou se existia ou não uma razão para pensar que a transferência podia ter lesado os interesses legítimos das pessoas em causa. A este respeito, constatou que a alegação da EFSA de que a divulgação da informação controvertida poderia causar prejuízo à vida privada e à integridade desses peritos era uma consideração de ordem geral não sustentada por nenhum elemento específico do caso vertente. O Tribunal de Justiça considerou, pelo contrário, que essa divulgação teria permitido, por si só, dissipar as suspeitas de parcialidade em causa ou teria dado aos peritos eventualmente afetados a oportunidade de contestarem, sendo caso disso pelos meios processuais disponíveis, o mérito dessas alegações de parcialidade. Atendendo a estes elementos, o Tribunal de Justiça anulou igualmente a decisão da EFSA (n.os 69 e 73).

* * *

Os acórdãos que figuram na presente ficha são indexados no Repertório de Jurisprudência nas rubricas 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07., 4.11.11.01.