TRIBUNAL DE JUSTIÇA
DA UNIÃO EUROPEIA

PT

Ficha temática
Proteção de dados pessoais

Direção da Investigação e Documentação

curia.europa.eu

Preâmbulo

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

Está consagrado no direito primário, nomeadamente no artigo 8.° da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»), bem como no artigo 16.°, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE). Este direito fundamental está, além disso, estreitamente relacionado com o direito ao respeito da vida privada e familiar consagrado no artigo 7.° da Carta.

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, revogada em 2018 [1], constituía o principal ato jurídico da União nesta matéria.

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 observar que, para ter em conta novas evoluções tecnológicas e comerciais, o legislador da União iniciou, em 2017, uma reapreciação desta diretiva [4], que está, atualmente, ainda em curso [5].

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

---

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 6).

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 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 A Comissão apresentou, em 10 de janeiro de 2017, uma proposta destinada a substituir esta diretiva por um regulamento relativo à privacidade e às comunicações eletrónicas.

5 Em 10 de fevereiro de 2021, o Conselho da União Europeia aprovou um mandato de negociação com vista à revisão das regras relativas à proteção da vida privada e da confidencialidade na utilização de serviços de comunicações eletrónicas, permitindo o início das negociações com o Parlamento Europeu. O texto da 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) está disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN.

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).

dados pessoais (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, cujas disposições são aplicáveis desde 6 de maio de 2018.

No que respeita ao tratamento de dados pessoais pelas instituições e órgãos da União, a respetiva proteção é nomeadamente assegurada, desde 11 de dezembro de 2018, pelo Regulamento (UE) 2018/1725 [8]. Para conseguir uma abordagem coerente da proteção de dados pessoais em toda a União, este regulamento visa alinhar tanto quanto possível as regras na matéria com o regime estabelecido pelo RGPD.

Por último, para responder aos desafios colocados pelas novas tecnologias, o legislador da União iniciou, em 2020, a adoção de novas medidas legislativas [9] que se articulam com as disposições do direito da UE em matéria de proteção de dados pessoais.

Tendo em conta a riqueza da jurisprudência do Tribunal de Justiça em matéria de proteção de dados pessoais, a presente ficha temática tem por objetivo apresentar uma seleção de acórdãos fundadores na matéria, bem como de acórdãos que contribuíram de forma significativa para o desenvolvimento desta jurisprudência, com especial destaque para os acórdãos proferidos pela Grande Secção do Tribunal de Justiça. Mais especificamente, esta ficha pretende abranger tanto a jurisprudência relativa à regulamentação geral em matéria de proteção de dados pessoais, decorrente da interpretação da Diretiva 95/46 e do RGPD, como a jurisprudência relativa à regulamentação setorial sobre, nomeadamente, o setor das comunicações eletrónicas e do direito penal. Por outro lado, pretende apresentar uma seleção de acórdãos relativos a regulamentações que se aplicam de forma transversal, salientando desde logo o papel determinante da Carta na construção da jurisprudência.

---

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 (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.º 45/2001 e a Decisão n.º 1247/2002/CE (JO 2018, L 295, p. 39).

9 Neste contexto, há que referir, em particular, três iniciativas legislativas: *i)* o Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados) (JO 2022, L 152, p. 1), e o Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828 (Regulamento dos Dados) (JO 2023, L 2854, p. 1); *ii)* um pacote legislativo sobre serviços e mercados digitais, constituído pelo Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) (JO 2022, L 277, p. 1), e o Regulamento 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022, relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais) (JO 2022, L 265, p. 1); e *iii)* a primeira proposta legislativa com vista à criação de um quadro regulamentar em matéria de inteligência artificial, que se concretizou por um regulamento sobre a inteligência artificial (JO 2024, L 1689).

Índice

I. O direito à proteção de dados pessoais reconhecido pela Carta dos Direitos Fundamentais da União Europeia

1. Conformidade do direito derivado da União com o direito à proteção de 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)

Nestes processos, 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 opunham-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 [10] e 259/2008 [11], que regem o financiamento da política agrícola comum e impõem a publicação de informações relativas às pessoas singulares beneficiárias do FEAGA e do FEADER.

Foi neste contexto que o Verwaltungsgericht Wiesbaden (Tribunal Administrativo de Wiesbaden, Alemanha) submeteu ao Tribunal de Justiça várias questões sobre a validade de certas disposições do Regulamento n.° 1290/2005 e do Regulamento n.° 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 de dados pessoais reconhecido pela Carta e a obrigação de transparência em matéria de fundos europeus, o Tribunal de Justiça 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.

---

10 Regulamento (CE) n.° 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.° 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).

11 Regulamento (CE) n.° 259/2008 da Comissão, de 18 de março de 2008, que estabelece as regras de execução do Regulamento (CE) n.° 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.° 908/2014 da Comissão, de 6 de agosto de 2014, que estabelece as normas de execução do Regulamento (UE) n.° 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).

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 de Justiça considerou que, embora numa sociedade democrática os contribuintes tenham o direito de ser 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.

Assim, o Tribunal de Justiça declarou inválidas certas disposições do Regulamento n.° 1290/2005, bem como o Regulamento n.° 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. 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.

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***)***

O presente acórdão tem origem nos pedidos de apreciação da validade da Diretiva 2006/24/CE relativa à conservação de dados, no que respeita aos direitos fundamentais ao respeito da vida privada e à proteção de dados pessoais, suscitados no âmbito de litígios nacionais perante um órgão jurisdicional irlandês e outro austríaco. 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 irlandês e austríaco interrogaram o Tribunal de Justiça 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 de Justiça 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 uma comunicação, o equipamento de comunicação dos utilizadores, bem como para localizar o equipamento de comunicação móvel, dados entre os quais figuram, designadamente, o nome e o endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário, bem como um endereço IP para os serviços Internet. Estes dados permitem, designadamente, saber quem 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 de Justiça 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 de dados pessoais garantidos pelos artigos 7.° e 8.° da Carta. Neste contexto, o Tribunal de Justiça 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 de Justiça 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 de 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 de Justiça observou que a conservação dos dados com vista à sua eventual transmissão às autoridades nacionais competentes respondia efetivamente a um objetivo de interesse geral, concretamente a luta contra a criminalidade grave, bem como, em última análise, a segurança pública.

No entanto, o Tribunal de Justiça 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 mesma impunha não estava suficientemente enquadrada de forma a garantir que se limitava ao estritamente necessário. 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. 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. 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.

Por outro lado, no que respeita às exigências decorrentes do artigo 8.°, n.° 3, da Carta, o Tribunal de Justiça 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, e também não impunha que os dados 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.

Acórdão de 21 de junho de 2022 (Grande Secção), Ligue des droits humains (C-817/19, EU:C:2022:491)

Os dados PNR (Passenger Name Record) são informações de reserva armazenadas pelas transportadoras aéreas nos seus sistemas de reservas e de controlo das partidas. A Diretiva PNR [12] obriga essas transportadoras a transferir os dados de qualquer passageiro que apanhe um voo extra-UE, operado entre um país terceiro e a União Europeia, para a Unidade de Informações de Passageiros (a seguir «UIP») do Estado-Membro de destino ou de partida do voo em causa, a fim de lutar contra as infrações terroristas e a criminalidade grave. Com efeito, os dados PNR assim transferidos são objeto de uma avaliação prévia pela UIP [13] e são, em seguida, conservados com vista a uma eventual avaliação posterior pelas autoridades competentes do Estado-Membro em causa ou de outro Estado-Membro. Os Estados-Membros podem decidir aplicar a diretiva também aos voos intra-EU [14].

A Ligue des droits humains interpôs na Cour constitutionnelle (Tribunal Constitucional, Bélgica) um recurso de anulação contra a lei belga que transpôs para o direito nacional a Diretiva PNR e a Diretiva API [15]. Segundo a recorrente, esta lei viola o direito ao

12 Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave (JO 2016, L 119, p. 132) (a seguir «Diretiva PNR»).

13 Esta avaliação prévia tem por objetivo identificar as pessoas relativamente às quais é necessário um exame mais aprofundado pelas autoridades competentes, tendo em conta o facto de que essas pessoas podem estar implicadas em infrações terroristas ou em criminalidade grave. A mesma é efetuada de forma sistemática e através de meios automatizados, confrontando os dados PNR com as bases de dados «úteis» ou tratando-os à luz dos critérios preestabelecidos no artigo 6, n.° 2, alínea a), e n.° 3, da Diretiva PNR.

14 Fazendo uso da possibilidade prevista no artigo 2.º da Diretiva PNR.

15 Diretiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras (JO 2004, L 261, p. 24) (a seguir «Diretiva API»). Esta diretiva regula a transmissão às autoridades nacionais competentes, pelas transportadoras aéreas, de informações prévias sobre passageiros (como o número e o tipo de documento de viagem utilizado e a nacionalidade), com vista a melhorar os controlos nas fronteiras e combater a imigração ilegal.

respeito da vida privada e à proteção de dados pessoais. A recorrente critica, por um lado, o caráter muito amplo dos dados PNR e, por outro, o caráter geral da recolha, da transferência e do tratamento desses dados. A lei viola igualmente a livre circulação de pessoas, uma vez que restabelece indiretamente controlos nas fronteiras, ao alargar o sistema PNR aos voos intra-UE e aos transportes efetuados por outros meios dentro da União.

Neste contexto, a Cour constitutionnelle belga submeteu ao Tribunal de Justiça um pedido de decisão prejudicial colocando-lhe questões relativas, nomeadamente, à validade da Diretiva PNR.

No seu acórdão, proferido pela Grande Secção, o Tribunal de Justiça confirma a validade da Diretiva PNR, na medida em que esta pode ser interpretada em conformidade com a Carta.

A este respeito, o Tribunal de Justiça declara que, uma vez que a interpretação feita pelo Tribunal de Justiça das disposições da Diretiva PNR à luz dos direitos fundamentais garantidos nos artigos 7.°, 8.°, 21.° e 52.°, n.° 1, da Carta [16] garante a conformidade desta diretiva com estes artigos, o exame das questões submetidas não revelou nenhum elemento suscetível de afetar a validade da referida diretiva.

A título preliminar, recorda que um ato da União deve ser interpretado, tanto quanto possível, de modo a não pôr em causa a sua validade e em conformidade com o direito primário no seu todo, nomeadamente, com as disposições da Carta, pelo que os Estados-Membros devem ter o cuidado de não se basear numa interpretação do mesmo que conflitue com os direitos fundamentais protegidos pelo ordenamento jurídico da União ou com outros princípios gerais reconhecidos por este ordenamento jurídico. No que diz respeito à Diretiva PNR, o Tribunal de Justiça esclarece que um número significativo dos seus considerandos e disposições impõem essa interpretação conforme, acentuando a importância dada pelo legislador da União, quando se refere a um elevado nível de proteção de dados, ao respeito integral pelos direitos fundamentais consagrados na Carta.

O Tribunal de Justiça declara que a Diretiva PNR comporta ingerências de uma certa gravidade nos direitos consagrados nos artigos 7.° e 8.° da Carta, na medida em que, nomeadamente, prevê a instituição de um regime de supervisão contínuo, não direcionado e sistemático que inclui a avaliação automatizada de dados pessoais de todas as pessoas que utilizam os serviços de transporte aéreo. Recorda que a possibilidade de os Estados-Membros justificarem esse tipo de ingerência deve ser

[16] Nos termos desta disposição, qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Além disso, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.

apreciado mensurando a sua gravidade e verificando que a importância do objetivo de interesse geral prosseguido se relaciona com essa gravidade.

O Tribunal de Justiça conclui que a transferência, o tratamento e a conservação dos dados PNR previstos nessa diretiva podem ser considerados limitados ao estritamente necessário para efeitos da luta contra o terrorismo e a criminalidade grave, desde que os poderes previstos na referida diretiva sejam objeto de uma interpretação restritiva. A este respeito, o acórdão hoje proferido esclarece nomeadamente que:

- O sistema estabelecido pela Diretiva PNR deve abranger apenas as informações claramente identificáveis e circunscritas às rubricas que figuram no seu anexo I, as quais se relacionam com o voo efetuado e o passageiro em causa, o que implica, para algumas das rubricas que figuram nesse anexo, que só estão abrangidas as informações aí expressamente previstas [17].
- A aplicação do sistema estabelecido pela Diretiva PNR deve limitar-se às infrações terroristas e apenas à criminalidade grave que apresente um nexo objetivo, pelo menos indireto, com o transporte aéreo de passageiros. No que se refere a essa criminalidade, a aplicação deste sistema não pode ser estendida às infrações que, embora preencham o critério previsto nesta diretiva relativamente ao limiar de gravidade e estejam, nomeadamente, previstas no seu anexo II, pertençam à criminalidade comum tendo em conta as especificidades do sistema penal nacional.
- A eventual extensão da aplicação da Diretiva PNR a todos ou a parte dos voos intra-UE, que um Estado-Membro pode decidir fazendo uso da faculdade prevista nesta diretiva, deve limitar-se ao estritamente necessário. Para o efeito, essa extensão deve poder ser objeto de uma fiscalização efetiva por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão é dotada de efeito vinculativo. A este respeito, o Tribunal de Justiça especifica que:
    - apenas na situação em que o referido Estado-Membro constate a existência de circunstâncias suficientemente concretas para considerar que está perante uma ameaça terrorista real e atual ou previsível, a aplicação desta diretiva a todos os voos intra-UE com proveniência de ou destino ao referido Estado-Membro, por um período limitado ao estritamente necessário mas renovável, não excede os limites do estritamente necessário [18].

[17] Assim, nomeadamente, «as informações sobre as modalidades de pagamento» (rubrica 6 do anexo) devem ser limitadas aos meios de pagamento e à faturação do bilhete de avião, excluindo qualquer outra informação sem relação direta com o voo, e as «observações gerais» (rubrica 12) só podem dizer respeito às informações expressamente enumeradas nesta rubrica, relativas aos passageiros menores.

[18] Com efeito, a existência de tal ameaça é, por si só, suscetível de estabelecer uma relação entre a transferência e o tratamento dos dados em causa e a luta contra o terrorismo. Por conseguinte, prever a aplicação da diretiva PNR a todos os voos intra-UE com proveniência ou destino ao Estado-Membro em causa, por um período limitado, não excede os limites do estritamente necessário, devendo a decisão que prevê essa aplicação poder ser controlada por um órgão jurisdicional ou por uma entidade administrativa independente.

- não havendo essa ameaça terrorista, a aplicação da referida diretiva não pode estender-se a todos os voos intra-UE, mas deve limitar-se aos voos intra-UE relativos, nomeadamente, a certas ligações aéreas ou planos de viagens ou ainda a certos aeroportos para os quais existem, segundo a apreciação do Estado-Membro em causa, indicações suscetíveis de justificar essa aplicação. O caráter estritamente necessário dessa aplicação aos voos intra-UE assim selecionados deve ser regularmente reexaminado, em função da evolução das condições que justificaram a sua seleção.

- Para efeitos da avaliação prévia dos dados PNR, que tem por objetivo identificar as pessoas relativamente às quais é exigido um exame mais aprofundado antes da sua chegada ou partida e que, num primeiro momento, é efetuada através de tratamentos automatizados, a UIP apenas pode, por um lado, confrontar esses dados com as bases de dados relativas a pessoas ou a objetos procurados ou que foram sinalizados [19]. Essas bases de dados devem ser não discriminatórias e ser usadas pelas autoridades competentes em relação à luta contra as infrações terroristas e a criminalidade grave que apresentem um nexo objetivo, pelo menos indireto, com o transporte aéreo de passageiros. Por outro lado, no que se refere à avaliação prévia à luz dos critérios preestabelecidos, a UIP não pode utilizar tecnologias de inteligência artificial no âmbito de sistemas de autoaprendizagem («*machine learning*»), suscetíveis de modificar, sem intervenção ou controlo humano, o processo de avaliação e, em especial, os critérios de avaliação em que se baseiam o resultado da aplicação deste processo e a ponderação dos mencionados critérios. Esses critérios devem ser determinados de forma que a sua aplicação vise, especificamente, os indivíduos relativamente aos quais possa haver uma suspeita razoável de participação em infrações terroristas ou em criminalidade grave e de modo a ter em conta os elementos «incriminatórios» e «ilibatórios», sem que simultaneamente dê lugar a discriminações diretas ou indiretas [20].

- Tendo em conta a taxa de erro inerente a esses tratamentos automatizados de dados PNR e a quantidade bastante significativa de resultados «falsos positivos», obtidos na sequência da sua aplicação em 2018 e 2019, a aptidão do sistema estabelecido pela Diretiva PNR para realizar os objetivos prosseguidos depende essencialmente do bom funcionamento da verificação dos resultados positivos, obtidos mediante esses tratamentos, que a UIP efetua, num segundo momento,

---

19 Isto é, bases de dados relativas a pessoas ou a objetos procurados ou alvo de um alerta, na aceção do artigo 6.°, n.° 3, alínea a), da diretiva PNR. Em contrapartida, análises a partir de bases de dados diversas podem assumir a forma de uma exploração de dados (*data mining*) e podem dar lugar a uma utilização desproporcionada desses dados, fornecendo os meios para estabelecer o perfil preciso das pessoas em causa pela simples razão de que estas têm a intenção de viajar de avião.

20 Os critérios preestabelecidos devem ser orientados em função dos objetivos, proporcionados e específicos, e ser revistos regularmente (artigo 6.°, n.° 4, da Diretiva PNR). A avaliação prévia de acordo com critérios preestabelecidos deve ser realizada de forma não discriminatória. Segundo o artigo 6.°, n.° 4, quarto período, esses critérios não podem, em caso algum, basear-se na raça ou na origem étnica de uma pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, na sua filiação sindical, na sua saúde, vida ou orientação sexual.

através de meios não automatizados. A este respeito, os Estados-Membros devem prever regras claras e precisas de forma a orientar e enquadrar a análise efetuada pelos agentes da UIP responsáveis por esse reexame individual para efeitos de assegurar o respeito integral dos direitos fundamentais consagrados nos artigos 7.°, 8.° e 21.° da Carta e, nomeadamente, garantir uma prática administrativa coerente no seio da UIP que respeite o princípio da não-discriminação. Em especial, devem assegurar que a UIP estabelece critérios de reexame objetivos que permitam aos seus agentes verificar, por um lado, se e em que medida uma concordância positiva *(hit)* diz efetivamente respeito a um indivíduo suscetível de estar implicado em infrações terroristas ou na criminalidade grave e, por outro lado, o caráter não discriminatório dos tratamentos automatizados. Neste contexto, o Tribunal de Justiça sublinha ainda que as autoridades competentes devem garantir que o interessado é capaz de compreender o funcionamento dos critérios de avaliação preestabelecidos e os programas que aplicam esses critérios, de forma a poder decidir, com total conhecimento de causa, se exerce ou não o seu direito à interposição de uma ação judicial. Do mesmo modo, no âmbito dessa ação, o juiz responsável pela fiscalização da legalidade da decisão adotada pelas autoridades competentes e, salvo os casos de ameaças à segurança do Estado, o próprio interessado, devem poder tomar conhecimento tanto do conjunto dos fundamentos como dos elementos de prova com base nos quais essa decisão foi tomada, incluindo os critérios de avaliação preestabelecidos e o funcionamento dos programas que aplicam esses critérios.

- A comunicação e a avaliação ulteriores dos dados PNR, ou seja, após a chegada ou a partida da pessoa em causa, só podem ser efetuadas com base em circunstâncias novas e elementos objetivos suscetíveis de fundar uma suspeita razoável de implicação dessa pessoa em criminalidade grave que apresente um nexo objetivo, pelo menos indireto, com o transporte aéreo de passageiros, ou que permitam considerar que esses dados poderiam, num caso concreto, dar uma contribuição efetiva à luta contra as infrações terroristas que apresentem esse nexo. A comunicação dos dados PNR para efeitos dessa avaliação ulterior deve, em princípio, salvo em caso de urgência devidamente justificado, ser subordinada a uma fiscalização prévia efetuada quer por um órgão jurisdicional, quer por uma autoridade administrativa independente, mediante pedido fundamentado das autoridades competentes, independentemente da questão de saber se esse pedido foi apresentado antes ou depois de decorrido o prazo de seis meses subsequente à transferência desses dados para a UIP [21].

[21] Nos termos do artigo 12.°, n.os 1 e 3, da Diretiva PNR, essa fiscalização só está expressamente prevista para os pedidos de comunicação de dados PNR apresentados depois de decorrido o prazo de seis meses subsequente à transferência desses dados para a UIP.

Acórdão de 22 de novembro de 2022 (Grande Secção), Luxembourg Business Registers (C-37/20 e C-601/20, EU:C:2022:912)

Para efeitos do combate e da prevenção do branqueamento de capitais e do financiamento do terrorismo, a Diretiva antibranqueamento [22] obriga os Estados-Membros a manterem um registo com informações sobre os beneficiários efetivos [23] das entidades societárias e outras pessoas coletivas constituídas no seu território. Na sequência de uma alteração desta diretiva pela Diretiva 2018/843 [24], , algumas dessas informações passaram a ter de estar acessíveis em todos os casos a qualquer membro do público em geral. Nos termos da Diretiva antibranqueamento conforme alterada (a seguir «Diretiva antibranqueamento alterada»), a legislação luxemburguesa instituiu um Registo dos beneficiários efetivos (a seguir «RBE») destinado a conservar e a disponibilizar um conjunto de informações sobre os beneficiários efetivos das entidades registadas cujo acesso está aberto a qualquer pessoa.

Neste contexto, foram interpostos dois recursos no tribunal d'arrondissement de Luxembourg (Tribunal de Primeira Instância do Luxemburgo), respetivamente por WM e pela Sovim SA, que contestam o indeferimento, pelo Luxembourg Business Registers, gestor do RBE, dos seus pedidos que visam impedir o acesso do público em geral a informações relativas, no primeiro processo, a WM na qualidade de beneficiário efetivo de uma sociedade civil imobiliária e, no segundo processo, ao beneficiário efetivo da Sovim SA. No âmbito destes dois processos, o tribunal d'arrondissement de Luxembourg (Tribunal de Primeira Instância do Luxemburgo), por ter dúvidas, nomeadamente, quanto à validade das disposições do direito da União que instauraram o sistema de acesso público às informações relativas aos beneficiários efetivos, submeteu ao Tribunal de Justiça uma questão prejudicial para apreciação de validade.

No seu acórdão, o Tribunal de Justiça, reunido em Grande Secção, declara inválida a Diretiva 2018/843 na parte em que alterou a Diretiva antibranqueamento no sentido de que os Estados-Membros devem assegurar que as informações sobre os beneficiários efetivos das entidades societárias e de outras pessoas coletivas constituídas no seu território sejam acessíveis em todos os casos a qualquer membro do público em geral [25].

---

22 Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, que altera o Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (JO 2015, L 141, p. 73; a seguir «Diretiva antibranqueamento»).

23 Nos termos do artigo 3.º, ponto 6, da Diretiva antibranqueamento, os beneficiários efetivos são as pessoas singulares que, em última instância, detêm a propriedade ou o controlo do cliente e/ou a pessoa ou pessoas singulares por conta de quem é realizada uma operação ou atividade.

24 Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE (JO 2018, L 156, p. 43).

25 Invalidade do artigo 1.º, ponto 15, alínea c), da Diretiva 2018/843, que altera o artigo 30.º, n.º 5, primeiro parágrafo, alínea c), da Diretiva antibranqueamento.

Em primeiro lugar, o Tribunal de Justiça constata que o acesso do público em geral às informações sobre os beneficiários efetivos, previsto na Diretiva antibranqueamento alterada, constitui uma ingerência grave nos direitos fundamentais de respeito pela vida privada e de proteção dos dados pessoais, consagrados, respetivamente, nos artigos 7.° e 8.° da Carta.

A este respeito, o Tribunal de Justiça observa que, uma vez que os dados em questão contêm informações sobre pessoas singulares identificadas, a saber, os beneficiários efetivos das entidades societárias e outras pessoas coletivas constituídas no território dos Estados-Membros, o acesso de qualquer membro do público em geral a estas informações afeta o direito fundamental de respeito pela vida privada. Além disso, a sua disponibilização ao público em geral constitui um tratamento de dados pessoais. O Tribunal de Justiça acrescenta que essa disponibilização ao público em geral constitui uma ingerência nos dois direitos fundamentais acima referidos, seja qual for a utilização posterior das informações comunicadas.

Quanto à gravidade desta ingerência, o Tribunal de Justiça salienta que, na medida em que as informações disponibilizadas ao público em geral dizem respeito à identidade do beneficiário efetivo, bem como à natureza e à extensão dos seus interesses efetivos detidos em entidades societárias ou noutras pessoas coletivas, estas informações são suscetíveis de permitir estabelecer um perfil relativo a certos dados pessoais de identificação, à situação patrimonial do interessado, bem como aos setores económicos, aos países e às empresas específicas em que este tenha investido. Além disso, estas informações tornam-se acessíveis a um número potencialmente ilimitado de pessoas, pelo que esse tratamento de dados pessoais também é suscetível de permitir que pessoas que, por razões alheias ao objetivo prosseguido por esta medida, procuram informar-se sobre a situação, nomeadamente material e financeira, de um beneficiário efetivo, acedam livremente às referidas informações. Esta possibilidade revela-se ainda mais fácil quando os dados possam ser consultados na Internet. Por outro lado, as potenciais consequências para os titulares dos dados resultantes de uma eventual utilização abusiva dos seus dados pessoais são agravadas pelo facto de que, depois de terem sido disponibilizados ao público em geral, esses dados podem não apenas ser livremente consultados, como podem também ser conservados e difundidos, tornando-se, assim, ainda mais difícil, ou mesmo ilusório, para essas pessoas defenderem-se eficazmente contra abusos.

Em segundo lugar, a título do exame da justificação da ingerência em causa, primeiro, o Tribunal de Justiça observa que, no caso em apreço, o princípio da legalidade foi respeitado. Com efeito, a restrição do exercício dos direitos fundamentais acima referidos que resulta do acesso do público em geral às informações sobre os beneficiários efetivos está prevista num ato legislativo, a saber, a Diretiva antibranqueamento alterada. Além disso, por um lado, esta diretiva precisa que essas informações devem ser suficientes, exatas e atuais, e enumera expressamente certos

dados aos quais deve ser concedido o acesso público. Por outro lado, estabelece as condições em que os Estados-Membros podem prever derrogações a esse acesso.

Segundo, o Tribunal de Justiça precisa que a ingerência em causa não viola o conteúdo essencial dos direitos fundamentais garantidos pelos artigos 7.° e 8.° da Carta. Embora seja certo que a Diretiva antibranqueamento alterada não contém uma enumeração exaustiva dos dados a que qualquer membro do público em geral deve poder aceder e que os Estados-Membros estão habilitados a permitir o acesso a informações adicionais, não é menos certo que só as informações adequadas sobre os beneficiários efetivos e os interesses efetivos detidos podem ser obtidas, conservadas e, por conseguinte, potencialmente tornadas acessíveis ao público, o que exclui, nomeadamente, informações que não tenham uma relação adequada com as finalidades da Diretiva antibranqueamento alterada. Ora, não se afigura que a disponibilização ao público em geral das informações que têm semelhante relação prejudique, de alguma forma, o conteúdo essencial dos direitos fundamentais visados.

Terceiro, o Tribunal de Justiça sublinha que, ao prever o acesso do público em geral às informações sobre os beneficiários efetivos, o legislador da União visa prevenir o branqueamento de capitais e o financiamento do terrorismo, criando, através de uma maior transparência, um ambiente menos suscetível de ser utilizado para esses fins, o que constitui um objetivo de interesse geral suscetível de justificar ingerências, inclusivamente graves, nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta.

Quarto, no âmbito da análise do caráter adequado, necessário e proporcionado da ingerência em causa, o Tribunal de Justiça constata que é certo que o acesso do público em geral às informações sobre os beneficiários efetivos é adequado para contribuir para a realização desse objetivo

Todavia, o Tribunal de Justiça entende que não se pode considerar que esta ingerência seja limitada ao estritamente necessário. Por um lado, a estrita necessidade da referida ingerência não pode ser demonstrada com base no facto de o critério do «interesse legítimo» de que, segundo a Diretiva antibranqueamento, na sua versão anterior à sua alteração pela Diretiva 2018/843, devia dispor qualquer pessoa que pretendesse aceder às informações sobre os beneficiários efetivos, ser difícil de aplicar e de a sua aplicação poder conduzir a decisões arbitrárias. Com efeito, a eventual existência de dificuldades para definir com precisão as hipóteses e as condições em que o público pode aceder a informações sobre os beneficiários efetivos não pode justificar que o legislador da União preveja o acesso do público em geral a essas informações.

Por outro lado, as explicações que figuram na Diretiva 2018/843 também não podem demonstrar a estrita necessidade da ingerência em causa [26]. Na medida em que,

[26] São referidas as explicações que figuram no considerando 30 da Diretiva 2018/843.

segundo estas explicações, se presume que o acesso do público em geral a informações sobre os beneficiários efetivos existe para permitir um maior escrutínio destas informações por parte da sociedade civil, nomeadamente a imprensa ou as organizações da sociedade civil, o Tribunal salienta que, tanto a imprensa como as organizações da sociedade civil que apresentem um nexo com a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo têm um interesse legítimo em aceder às informações em questão. Sucede o mesmo com as pessoas que pretendem conhecer a identidade dos beneficiários efetivos de uma entidade societária ou de outra pessoa coletiva pelo facto de poderem efetuar transações com estas, ou ainda as instituições financeiras e as autoridades envolvidas na luta contra infrações em matéria de branqueamento de capitais ou de financiamento do terrorismo.

Além disso, a ingerência em causa também não apresenta um caráter proporcionado. A este respeito, o Tribunal constata que as regras materiais que enquadram esta ingerência não correspondem à exigência de clareza e de precisão. Com efeito, a Diretiva antibranqueamento alterada prevê o acesso de qualquer membro do público em geral «pelo menos» aos dados nela referidos e confere aos Estados-Membros a faculdade de permitirem o acesso a informações adicionais, incluindo, «pelo menos», a data de nascimento ou os contactos do beneficiário efetivo em questão. Ora, através da utilização da expressão «pelo menos», esta diretiva autoriza a disponibilização ao público de dados que não estão suficientemente definidos nem são suficientemente identificáveis.

Acresce que, no que respeita à ponderação da gravidade desta ingerência com a importância do objetivo de interesse geral visado, o Tribunal de Justiça reconhece que, atendendo à sua importância, este objetivo é suscetível de justificar ingerências, inclusivamente graves, aos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta.

No entanto, por um lado, o combate ao branqueamento de capitais e ao financiamento do terrorismo incumbe prioritariamente às autoridades públicas e às entidades, como as instituições de crédito ou as instituições financeiras, às quais, devido às suas atividades, são impostas obrigações específicas nesta matéria. Por este motivo, a Diretiva antibranqueamento alterada prevê que as informações sobre os beneficiários efetivos devem ser acessíveis, em todos os casos, às autoridades competentes e às unidades de informação financeira, sem restrições, bem como às entidades obrigadas, no âmbito da diligência quanto à clientela [27].

Por outro lado, quando comparado com o regime anterior que previa, além do acesso das autoridades competentes e de certas entidades às informações sobre os beneficiários efetivos, o acesso de quaisquer pessoas ou organizações que pudessem provar possuir um interesse legítimo, o regime introduzido pela Diretiva 2018/843

[27] Artigo 30.°, n.° 5, primeiro parágrafo, alíneas a) e b), da Diretiva antibranqueamento alterada.

representa uma violação consideravelmente mais grave dos direitos fundamentais garantidos pelos artigos 7.° e 8.° da Carta, sem que esse agravamento seja compensado pelos eventuais benefícios que poderiam resultar deste último regime em relação ao primeiro no que se refere ao combate ao branqueamento de capitais e ao financiamento do terrorismo.

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)

Na sequência do Acórdão Digital Rights Ireland e Seitlinger e o., que declarou inválida a Diretiva 2006/24 (v. *supra*), o Tribunal de Justiça 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 de Justiça 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 de Justiça 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 de Justiça, tal regulamentação excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática, como exige o referido artigo 15.°, n.° 1, lido à luz dos artigos acima referidos da Carta.

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.

O Tribunal de Justiça 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.

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

1. Âmbito de aplicação da regulamentação geral

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 (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 [28], 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 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 [29] que aprovava a celebração de um acordo entre a Comunidade Europeia e os Estados Unidos 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 de Justiça que anulasse as duas decisões acima referidas, alegando, nomeadamente, que a decisão de adequação tinha sido adotada *ultra vires*, que o artigo 95.° CE (atual artigo 114.° 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 de Justiça 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

[28] 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).

[29] 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).

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 de Justiça, 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.

A este respeito, o Tribunal de Justiça 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 de Justiça concluiu que a decisão de adequação não era abrangida pelo âmbito de aplicação da diretiva, uma vez que dizia respeito a um tratamento de dados pessoais que estava excluído da mesma. Por conseguinte, o Tribunal de Justiça anulou a decisão de adequação.

No que se refere à decisão do Conselho, o Tribunal de Justiça 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 de Justiça anulou a decisão do Conselho que aprovou a celebração do acordo.

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, datadas 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 a sua reclamação, essa pessoa 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 se ordenasse à

Google Spain ou à Google que suprimissem ou ocultassem 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 indeferiu 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 aos mesmos no futuro. Tendo as referidas sociedades interposto dois recursos na Audiencia Nacional (Audiência Nacional, Espanha), com vista a obter a anulação da decisão da AEPD, o órgão jurisdicional espanhol submeteu uma série de questões ao Tribunal de Justiça.

Neste acórdão, o Tribunal de Justiça pronunciou-se igualmente sobre o âmbito de aplicação territorial da Diretiva 95/46.

Assim, o Tribunal de Justiça 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, embora 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.

Com efeito, nestas circunstâncias, as atividades do operador do motor de busca e as do seu estabelecimento situado num Estado-Membro, embora sejam 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 esse motor é, ao mesmo tempo, o meio que permite realizar essas atividades.

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 de dados pessoais, este último declarou que F. Ryneš tinha violado as regras em matéria de proteção dos dados pessoais e aplicou-lhe uma coima.

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 de Justiça considerou 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, instalado por uma pessoa singular na sua casa de família, para proteger os bens, a saúde e a vida dos proprietários da casa, sistema esse que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas.

A este respeito, o Tribunal de Justiça recordou que a proteção do direito fundamental à vida privada, garantido pelo artigo 7.° da Carta, exige que as derrogações à proteção dos dados pessoais e as respetivas limitações ocorram nos limites do estritamente necessário. Na medida em que as disposições da Diretiva 95/46, que regulam o tratamento de dados pessoais suscetível de pôr em causa as liberdades fundamentais, em especial o direito à vida privada, têm, necessariamente, de 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. 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.

Acórdão de 16 de janeiro de 2024 (Grande Secção), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Para examinar uma eventual influência política sobre o Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Serviço Federal para a Proteção da Constituição e a Luta contra o Terrorismo, Áustria) [30], a Nationalrat (Assembleia Nacional, Áustria) constituiu uma comissão de inquérito (a seguir «comissão de inquérito BVT»). Esta comissão ouviu WK como testemunha. Apesar do seu pedido de anonimização, a ata da sua audição, que mencionava os seus apelidos e nomes próprios completos, foi publicada no sítio Internet do Parlament Österreich (Parlamento Austríaco). Alegando que essa divulgação da sua identidade era contrária ao RGPD e à legislação austríaca, WK apresentou uma reclamação na Österreichische Datenschutzbehörde (Autoridade para a Proteção de Dados, Áustria) (a seguir

[30] Em 1 de dezembro de 2021, a «Direktion Staatsschutz und Nachrichtendienst» (Direção da Segurança do Estado e dos Serviços de Informações, Áustria) sucedeu a esta entidade.

«Datenschutzbehörde»). Por Decisão de 18 de setembro de 2019, a Datenschutzbehörde declarou-se incompetente para se pronunciar sobre a reclamação, explicando que o princípio da separação de poderes excluía que, enquanto órgão do poder executivo, pudesse fiscalizar a comissão de inquérito BVT, que faz parte do poder legislativo.

Na sequência da decisão do Bundesverwaltungsgericht (Tribunal Administrativo Federal, Áustria), que deu provimento ao recurso de WK e anulou a decisão da Datenschutzbehörde, esta última interpôs, no Supremo Tribunal Administrativo, um recurso de «Revision» da decisão do Tribunal Administrativo Federal.

Neste contexto, o órgão jurisdicional de reenvio interrogou o Tribunal de Justiça sobre a questão de saber se as atividades de uma comissão de inquérito instituída pelo Parlamento de um Estado-Membro estão abrangidas pelo âmbito de aplicação do RGPD e se este regulamento é aplicável quando essas atividades dizem respeito à proteção da segurança nacional.

Em primeiro lugar, o Tribunal de Justiça recorda que o artigo 2.°, n.° 2, alínea a), do RGPD, que prevê que este regulamento não se aplica ao tratamento de dados pessoais efetuado no exercício de atividades não sujeitas à aplicação do direito da União, tem por único objetivo excluir do seu âmbito de aplicação os tratamentos efetuados pelas autoridades estatais no âmbito de uma atividade que visa preservar a segurança nacional ou que se enquadra na mesma categoria. Assim, o simples facto de uma atividade ser própria do Estado ou de uma autoridade pública não é suficiente para que esta exceção seja automaticamente aplicável a tal atividade

Esta interpretação, que decorre da falta de distinção em função da identidade do autor do tratamento em causa, é confirmada pelo artigo 4.o, ponto 7, do RGPD [31].

O Tribunal de Justiça precisa que a natureza parlamentar da comissão de inquérito BVT não implica que as suas atividades estejam excluídas do âmbito de aplicação do RGPD. Com efeito, a exceção prevista no artigo 2.°, n.° 2, alínea a), deste regulamento refere-se apenas a categorias de atividades que, em razão da sua natureza, não estão abrangidas pelo âmbito de aplicação do direito da União, e não a categorias de pessoas. Por conseguinte, a circunstância de o tratamento de dados pessoais ser efetuado por uma comissão de inquérito instituída pelo Parlamento de um Estado-Membro no exercício do seu poder de fiscalização do poder executivo não permite, enquanto tal, demonstrar que esse tratamento é efetuado no contexto de atividades não sujeitas à aplicação do direito da União.

Em segundo lugar, o Tribunal de Justiça recorda que, embora incumba aos Estados-Membros definirem os seus interesses essenciais de segurança e adotarem as

[31] Este artigo define o conceito de «responsável pelo tratamento» como «a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais».

medidas adequadas para a salvaguardar [32],o simples facto de uma medida nacional ter sido adotada para efeitos da proteção da segurança nacional não pode levar à inaplicabilidade do direito da União e dispensar os Estados-Membros do respeito necessário desse direito. Ora, a exceção prevista no artigo 2.°, n.° 2, alínea a), do RGPD refere-se apenas a categorias de atividades que, em razão da sua natureza, não estão abrangidas pelo âmbito de aplicação do direito da União. A este respeito, a circunstância de o responsável pelo tratamento ser uma autoridade pública cuja atividade principal é assegurar a segurança nacional não basta, enquanto tal, para excluir do âmbito de aplicação do RGPD os tratamentos de dados pessoais que efetua no âmbito das suas outras atividades.

No caso em apreço, a fiscalização política efetuada pela comissão de inquérito BVT não parece constituir, enquanto tal, uma atividade que visa preservar a segurança nacional ou que se enquadra na mesma categoria. Por conseguinte, sem prejuízo de verificação pelo órgão jurisdicional de reenvio, esta atividade não está fora do âmbito de aplicação do RGPD.

No entanto, uma comissão de inquérito parlamentar pode ter acesso a dados pessoais que, por razões de segurança nacional, devem beneficiar de uma proteção especial. A este respeito, podem ser estabelecidas limitações, através de medidas legislativas, às obrigações e aos direitos decorrentes do RGPD, para assegurar, designadamente, a segurança do Estado [33]. Assim, com este fundamento, podem ser justificadas limitações no que respeita à recolha de dados pessoais, à informação dos titulares dos dados e ao seu acesso aos referidos dados ou ainda à divulgação desses dados, sem o consentimento dos titulares dos dados, a pessoas que não sejam o responsável pelo tratamento, desde que respeitem a essência dos direitos e liberdades fundamentais dos titulares dos dados e constituam uma medida necessária e proporcionada numa sociedade democrática.

O Tribunal de Justiça observa, todavia, que não resulta das informações postas à sua disposição que a comissão de inquérito BVT tenha alegado que a divulgação dos dados pessoais em causa era necessária para a salvaguarda da segurança nacional e se baseava numa medida legislativa nacional prevista para esse efeito, o que incumbe, sendo caso disso, ao órgão jurisdicional de reenvio verificar.

[32] Em conformidade com o artigo 4.°, n.° 2, TUE.
[33] Segundo o artigo 23.° do RGPD.

2. Conceito de «dados pessoais»

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

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, para se proteger de ataques e permitir a tramitação de ações penais contra os «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. Diferentemente dos endereços IP estáticos, os endereços IP dinâmicos não permitem, *a priori,* estabelecer a relação, 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 de Justiça 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 de Justiça começou por salientar 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.

Por conseguinte, o Tribunal de Justiça 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 dispõe dessa pessoa.

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 apresentou, ao abrigo do artigo 4.° da Lei de proteção de dados, um pedido de acesso a todos os dados pessoais que lhe diziam respeito detidos pela Câmara dos técnicos oficiais de contas. Esta última comunicou 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.

Uma vez 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, interrogou o Tribunal de Justiça sobre 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 relacionadas com essas respostas constituem dados pessoais na aceção desta disposição.

Em primeiro lugar, o Tribunal de Justiça salientou 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 quando 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, imputar-lhe as suas respostas.

Em segundo lugar, o Tribunal de Justiça 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.

Em terceiro lugar, no que respeita às anotações do examinador relativas às respostas do candidato, o Tribunal de Justiça 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. Por outro lado, as referidas anotações têm precisamente como finalidade documentar a avaliação, feita pelo examinador, da prestação do candidato e são suscetíveis de ter efeitos para este último.

Em quarto lugar, o Tribunal de Justiça 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 artigo 12.°, alínea b), desta diretiva. 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 isso 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 de Justiça 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.

Tendo em conta estes elementos, o Tribunal de Justiça 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 eventuais anotações do examinador relativas a essas respostas constituem dados pessoais, na aceção do artigo 2.°, alínea a), da Diretiva 95/46.

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 de Justiça 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 de Justiça declarou que a operação que consiste na referência, numa página 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. Com efeito, tal tratamento de dados pessoais, efetuado para o exercício de atividades de voluntariado ou religiosas, não é abrangido por nenhuma das exceções ao âmbito de aplicação da diretiva, uma vez que não se enquadra 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.

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

Neste acórdão (v. igualmente rubrica II.1, intitulada «Âmbito de aplicação da regulamentação geral»), o Tribunal de Justiça teve a oportunidade de precisar o conceito de «tratamento de dados pessoais» na Internet à luz da Diretiva 95/46.

Assim, o Tribunal de Justiça declarou 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. Além disso, o Tribunal de Justiça recordou 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.

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

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 desta 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 dessa 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, as quais constavam de, pelo menos, uma das suas publicações consagradas à atividade de pregação.

O Tribunal de Justiça 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.

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 [34], 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 no Latvijas Republikas Satversmes tiesa (Tribunal Constitucional, Letónia),

[34] Artigo 14.°[1], n.° 2, da Ceļu satiksmes likums (Lei da Circulação Rodoviária), de 1 de outubro de 1997 (Latvijas Vēstnesis, 1997, n.° 274/276).

para que este examinasse a conformidade dessa legislação com o direito ao respeito pela vida privada.

O Tribunal Constitucional considerou que, no âmbito da sua apreciação deste direito constitucional, deve ter em conta o RGPD. 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 este 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» [35], para o qual o RGPD prevê uma proteção acrescida devido à particular sensibilidade dos dados em causa.

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.

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 [36]. 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 têm 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.

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 [37]. Com efeito, o Tribunal de Justiça declara que, quando efetua a referida comunicação, não se pode considerar que a CSDD seja uma «autoridade competente» dessa natureza [38].

---

35 Artigo 10.º do RGPD.

36 Artigo 2.º, n.º 2, alínea a), do RGPD.

37 Artigo 2.º, n.º 2, alínea d), do RGPD.

38 Artigo 3.º, n.º 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,

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» [39], 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», uma vez 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 de Justiça 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.

Acórdão de 5 de dezembro de 2023 (Grande Secção), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Em 2020, para melhor gerir a pandemia de COVID-19, as autoridades lituanas decidiram organizar a aquisição de uma aplicação informática móvel. Esta aplicação devia contribuir para um acompanhamento epidemiológico, permitindo registar e acompanhar dados das pessoas expostas ao vírus da COVID-19.

Para o efeito, o Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Centro Nacional de Saúde Pública do Ministério da Saúde, Lituânia, a seguir «CNSP»), encarregado desta aquisição, contactou a sociedade UAB «IT sprendimai sėkmei» (a seguir «sociedade ITSS»), pedindo-lhe para proceder à criação dessa aplicação móvel. Em seguida, foram enviadas a essa sociedade, pelos funcionários do

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).

39 Artigo 10.º do RGPD.

CNSP, mensagens de correio eletrónico relativas nomeadamente às questões que deviam constar nessa aplicação.

Entre abril e maio de 2020, a aplicação móvel criada pela sociedade ITSS foi colocada à disposição do público. Por conseguinte, 3 802 pessoas utilizaram-na e forneceram diferentes dados, pedidos por essa aplicação, que lhes diziam respeito. No entanto, devido a falta de financiamento, o CNSP não adjudicou à sociedade ITSS nenhum contrato público com vista à aquisição oficial da sua aplicação móvel e pôs termo ao respetivo procedimento.

Entretanto, a autoridade nacional de controlo iniciou uma investigação relativa ao tratamento de dados pessoais resultante da utilização dessa aplicação. Por decisão desta autoridade, adotada no termo da investigação, foram aplicadas coimas quer ao CNSP quer à sociedade ITSS, considerada responsável conjunta pelo tratamento.

O CNSP contestou esta decisão no Vilniaus apygardos administracinis teismas (Tribunal Administrativo Regional de Vílnius, Lituânia). Por ter dúvidas quanto à interpretação de várias disposições do RGPD, esse órgão jurisdicional submeteu ao Tribunal de Justiça um pedido de decisão prejudicial.

No seu acórdão, o Tribunal de Justiça, reunido em Grande Secção, fornece esclarecimentos, entre outros, sobre o conceito de «tratamento». A este respeito, indica que a utilização de dados pessoais para efeitos de testes informáticos de uma aplicação móvel constitui um tratamento. No entanto, não é assim se tais dados tiverem sido tornados anónimos de modo que a pessoa à qual tais dados dizem respeito não seja ou já não seja identificável ou se estiverem em causa dados fictícios que não dizem respeito a uma pessoa singular existente.

Com efeito, por um lado, a questão de saber se são utilizados dados pessoais para testes informáticos ou para outro fim é irrelevante para a qualificação da operação como «tratamento». Por outro lado, só um tratamento que vise dados pessoais pode ser qualificado de «tratamento», na aceção do RGPD. Ora, os dados fictícios ou anónimos não constituem dados pessoais.

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 processo (v. igualmente rubrica II.3., intitulada «Conceito de “tratamento de dados pessoais”»), o Tribunal de Justiça 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 de Justiça 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 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.

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 rubricas II.3. e II.4., intituladas «Conceito de "tratamento de dados pessoais" e «Conceito de "ficheiro de dados pessoais"»), o Tribunal de Justiça pronunciou-se a respeito da responsabilidade de uma comunidade religiosa relativamente aos tratamentos de dados pessoais efetuados no âmbito de uma atividade de pregação porta-a-porta organizada, coordenada e promovida por esta comunidade.

Assim, o Tribunal de Justiça 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 propósito, 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.

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

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 de Justiça precisou o conceito de «responsável pelo tratamento» de dados pessoais. A este respeito, considerou 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. Por este facto, segundo o Tribunal de Justiça, este administrador deve ser qualificado de responsável na União, conjuntamente com a Facebook Ireland (filial da sociedade americana Facebook na União Europeia), por esse tratamento, na aceção do artigo 2.°, alínea d), da Diretiva 95/46.

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

Neste processo, o Tribunal de Justiça teve a oportunidade 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 parece ter como consequência que, quando um visitante consulta o sítio Internet da Fashion ID, dados pessoais desse visitante são transmitidos à Facebook Ireland. Afigura-se que esta transmissão é efetuada sem que o referido visitante dela esteja 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 litígio, o Oberlandesgericht Düsseldorf (Tribunal Regional Superior de Düsseldorf, Alemanha) pediu ao Tribunal de Justiça que procedesse à interpretação de várias disposições da Diretiva 95/46.

O Tribunal de Justiça começou por constatar 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 de Justiça, afigura-se, à partida, que a Fashion ID não determina 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 deste artigo 2.°, alínea d).

Além disso, o Tribunal de Justiça 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.

Por último, o Tribunal de Justiça 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 referido administrador, devendo, no entanto, a informação que este tem de 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.

Acórdão de 5 de dezembro de 2023 (Grande Secção), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Neste processo (v. igualmente rubrica II.3, intitulada «Conceito de "tratamento de danos pessoais"»), o Tribunal de Justiça salienta que uma entidade que encarregou uma empresa de desenvolver uma aplicação informática móvel e que, nesse contexto, participou na determinação das finalidades e dos meios do tratamento dos dados pessoais realizado através desta aplicação pode ser considerada responsável pelo tratamento [40]. Esta consideração não pode ser posta em causa pelo facto de a entidade não ter procedido, ela própria, a operações de tratamento de tais dados, não ter dado explicitamente o seu acordo para a realização das operações concretas desse tratamento ou para a disponibilização ao público da referida aplicação móvel e não ter adquirido esta mesma aplicação móvel, a menos que, antes dessa disponibilização ao público, a referida entidade se tenha expressamente oposto a ela e ao tratamento dos dados pessoais que daí resultou.

[40] Na aceção do artigo 4.°, ponto 7, do RGPD.

6. Conceito de «responsável conjunto pelo tratamento»

Acórdão de 5 de dezembro de 2023 (Grande Secção), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Neste processo (v. igualmente rubricas II.3 e II.5, intituladas «Conceito de "tratamento de danos pessoais"» e «Conceito de "responsável pelo tratamento de dados pessoais"»), o Tribunal de Justiça observa que a qualificação de duas entidades como sendo responsáveis conjuntas pelo tratamento não pressupõe nem a existência de um acordo entre essas entidades quanto à determinação das finalidades e dos meios do tratamento dos dados pessoais em causa, nem a existência de um acordo que fixe as condições relativas à responsabilidade conjunta pelo tratamento. É certo que, por força do RGPD [41], os responsáveis conjuntos pelo tratamento devem, por acordo entre si, determinar de modo transparente as respetivas obrigações para efeitos de assegurar o respeito das exigências deste regulamento. Todavia, a existência de semelhante acordo constitui não uma condição prévia para que duas ou mais entidades sejam qualificadas de «responsáveis conjuntas pelo tratamento», mas uma obrigação que o RGPD impõe aos responsáveis conjuntos pelo tratamento, uma vez assim qualificados, para assegurar o respeito das exigências deste regulamento que impendem sobre elas. Assim, esta qualificação decorre do simples facto de várias entidades terem participado na determinação das finalidades e meios do tratamento.

Quanto à determinação conjunta, pelas entidades em causa, das finalidades e dos meios do tratamento, o Tribunal de Justiça especifica que a sua participação nesta determinação pode assumir diferentes formas e resultar quer de uma decisão comum quer de decisões convergentes dessas entidades. Ora, neste último caso, estas decisões devem complementar-se de tal forma que cada uma delas tenha um efeito concreto na determinação das finalidades e meios do tratamento.

7. Requisitos de licitude de um tratamento de dados pessoais

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

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, bem como pelas autoridades

[41] Artigo 26.°, n.° 1, do RGPD, lido à luz do seu considerando 79.

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, cidadão 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 cidadãos 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 de Justiça recordou, antes de mais, 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 encarregadas 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.

Quanto ao conceito de «necessidade» do tratamento na aceção do artigo 7.°, alínea e), da Diretiva 95/46, o Tribunal de Justiça 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, constatou que um sistema de tratamento de dados pessoais só é conforme ao direito da União se contiver unicamente os dados necessários para a 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 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.

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

dos dados pessoais relativos unicamente aos cidadãos da União, 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.

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

Neste acórdão (v. igualmente rubrica II.2., intitulada «Conceito de "dados pessoais"») o Tribunal de Justiça 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 lícito se for necessário para a realização do interesse legítimo prosseguido pelo responsável pelo tratamento ou pelo 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.

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 a 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 por esta no âmbito da cobrança de impostos e cuja atualização era assegurada pela Direção de Finanças e 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 de Justiça a questão de saber, nomeadamente, se o direito ao respeito da vida privada e familiar, do domicílio e das comunicações, consagrado no artigo 7.°, e o direito à proteção de dados pessoais, consagrado no artigo 8.° da Carta, podiam 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, de modo que a obtenção de dados pessoais pelas autoridades públicas para combater a fraude fiscal poderia, em si mesma, constituir um risco.

O Tribunal de Justiça 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 aquele a que procedeu com a elaboração de uma lista de pessoas como a que está em causa 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, a elaboração dessa lista e a inscrição do nome das pessoas em causa sejam efetivamente adequadas e necessárias para alcançar os objetivos prosseguidos e haja indícios suficientes para presumir que a inscrição das pessoas em causa na lista é justificada e, por outro, estejam cumpridos todos os requisitos de licitude deste tratamento de dados pessoais impostos pela Diretiva 95/46.

A este respeito, o Tribunal de Justiça declarou que incumbe ao órgão jurisdicional de reenvio verificar se a elaboração da lista controvertida é necessária para a execução das missões de interesse público em causa no processo principal, atendendo, designadamente, à finalidade exata da elaboração 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 elaboração 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.

Além disso, o Tribunal de Justiça 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, essa 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.

Por outro lado, o Tribunal de Justiça 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 para a salvaguarda 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.

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

A Orange România presta serviços de telecomunicações móveis no mercado romeno. Em 28 de março de 2018, a Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Autoridade Nacional de Supervisão do Tratamento de 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 de Justiça recorda, antes de mais, que o direito da União [42] 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 [43]. A este respeito, o consentimento não é validamente dado em caso de silêncio, de opções validadas por defeito ou de inatividade.

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.

[42] Artigo 7.°, da Diretiva 95/46 e artigo 6.°, do RGPD.
[43] Artigo 2.°, alínea h), da Diretiva 95/46 e artigo 4, ponto 11, do RGPD.

O Tribunal de Justiça 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.

Cabe igualmente ao órgão jurisdicional nacional, segundo o Tribunal de Justiça, 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 de Justiça 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 de Justiça, 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 a referida 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.

O Tribunal de Justiça 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 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, para recusar dar o seu consentimento, preencha um formulário suplementar onde fique registada essa recusa.

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 de Justiça 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 de Justiça 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 de Justiça, nem o direito do público de aceder aos documentos oficiais nem o direito à liberdade de informação justificam tal legislação.

Neste contexto, o Tribunal de Justiça 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» [44]. 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.

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.

Por outro lado, por razões idênticas, o Tribunal de Justiça 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.

Por último, o Tribunal de Justiça 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 Justiça 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.

---

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

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

1. Tratamento de dados pessoais no setor das comunicações eletrónicas

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

Neste processo, estava em causa o indeferimento, por um juiz de instrução espanhol, de um pedido apresentado no âmbito 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 , com efeito, o acesso aos dados de identificação só ser 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 contexto de um processo de instrução penal, é abrangido pelo âmbito de aplicação da Diretiva 2002/58, o Tribunal de Justiça 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 de Justiça 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 este objetivo à luta contra as infrações graves, mas visa as «infrações penais» em geral.

Neste contexto, o Tribunal de Justiça precisou que, embora, no seu Acórdão Tele2 Sverige e Watson e o [45]., tivesse declarado que apenas a luta contra a criminalidade grave pode justificar que as autoridades públicas acedam a dados pessoais que são conservados pelos prestadores 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.

Neste caso concreto, o Tribunal de Justiça 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 de Justiça concluiu daí 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».

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)

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 de Justiça 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 para a salvaguarda da segurança nacional e para a 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.,

[45] Acórdão do Tribunal de Justiça de 21 de dezembro de 2016, *Tele2 Sverige e Watson e* o. (C-203/15 e C-698/15, EU:C:2016:970).

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 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 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.

Em seguida, o Tribunal de Justiça recorda que a Diretiva 2002/58 [46] 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 esta 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 [47], no respeito dos princípios gerais do direito da União, entre os quais figura o princípio da proporcionalidade, e dos direitos fundamentais garantidos pela Carta [48].

Neste contexto, o Tribunal de Justiça considera, por um lado, no processo Privacy International, que a Diretiva 2002/58, lida à luz da Carta, se opõe a uma regulamentação nacional que impõe aos prestadores 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.°, n.° 1, do RGPD, lido à luz da Carta, no sentido de que se opõe a uma

[46] Artigo 15.°, n.os 1 e 3, da Diretiva 2002/58.
[47] Artigo 5.°, n.° 1, da Diretiva 2002/58.
[48] Em especial, os artigos 7.°, 8.° e 11.°, bem como o artigo 52.°, n.° 1, da Carta.

regulamentação nacional que impõe aos fornecedores 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.

Em contrapartida, o Tribunal de Justiça entende 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 prestadores de serviços de comunicações eletrónicas que conservem de forma generalizada e 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, com vista a 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.

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, esta 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 ofensas já tenham sido constatadas ou quando se possa razoavelmente suspeitar da sua existência.

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 prestadores 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.

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 prestadores 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.

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. H. K. foi condenada, por um tribunal de primeira instância, numa pena privativa de liberdade de dois anos pela prática destes crimes. 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 da prestação de serviços de comunicações eletrónicas. O Riigikohus (Supremo Tribunal, Estónia), no qual H. K. interpôs recurso de cassação, manifestou dúvidas quanto à compatibilidade com o direito da União [49] das condições em que os serviços de inquérito tiveram acesso a esses dados.

[49] Mais precisamente, com o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.°, 11.° e 52.°, n.° 1, da Carta.

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 das pessoas em causa. Assim, o órgão jurisdicional de reenvio interrogou-se sobre 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 quando o referido período é muito curto ou 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 [50]., 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 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 de Justiça, 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 de Justiça 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.

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 de Justiça 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 causa 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

[50] Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970, n.º 120).

prevenção, de investigação, de deteção e de repressão de infrações penais em geral seja suscetível de justificar esse acesso.

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 para dirigir uma instrução penal, o Tribunal de Justiça 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.

Segundo o Tribunal de Justiça, para 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.

A este respeito, o Tribunal de Justiça 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.

Segundo o Tribunal de Justiça, 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.

Acórdão de 5 de abril de 2022 (Grande Secção), Commissioner of An Garda Síochána e o. (C-140/20, EU:C:2022:258)

No presente processo, o pedido de decisão prejudicial foi apresentado pela Supreme Court (Supremo Tribunal, Irlanda) no âmbito de uma ação cível intentada por uma pessoa condenada a prisão perpétua por um homicídio cometido na Irlanda. Esta última contestava a compatibilidade com o direito da União de certas disposições da lei nacional relativa à conservação de dados gerados no contexto das comunicações eletrónicas. Ao abrigo desta lei, tinham sido conservados pelos prestadores de serviços de comunicações eletrónicas e tornados acessíveis às autoridades de polícia dados de tráfego e dados de localização relativos às chamadas telefónicas da pessoa condenada. As dúvidas manifestadas pelo órgão jurisdicional de reenvio diziam respeito, nomeadamente, à compatibilidade com a Diretiva 2002/58, lida à luz da Carta, de um regime de conservação generalizada e indiferenciada desses dados, relacionado com a luta contra a criminalidade grave.

No seu acórdão, proferido em Grande Secção, o Tribunal de Justiça confirma, precisando o seu alcance, a jurisprudência resultante do Acórdão La Quadrature du Net e o [51], recordando que a conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização relativos às comunicações eletrónicas não é autorizada para efeitos da luta contra a criminalidade grave e de prevenção das ameaças graves contra a segurança pública. Confirma igualmente a jurisprudência resultante do Acórdão Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) [52], nomeadamente quanto à obrigação de sujeitar o acesso das autoridades nacionais competentes aos referidos dados conservados a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente, relativamente a um agente de polícia.

O Tribunal de Justiça considera, em primeiro lugar, que a Diretiva 2002/58, lida à luz da Carta, se opõe a medidas legislativas que preveem, a título preventivo, para efeitos da

[51] Acórdão de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791).
[52] Acórdão de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152).

luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização. Com efeito, tendo em conta, por um lado, os efeitos dissuasivos sobre o exercício dos direitos fundamentais [53] que essa conservação pode acarretar e, por outro, a gravidade da ingerência que a mesma implica, essa conservação deve constituir a exceção e não a regra ao sistema instituído por esta diretiva, de modo que esses dados não possam ser objeto de uma conservação sistemática e contínua. A criminalidade, ainda que particularmente grave, não pode ser equiparada a uma ameaça contra a segurança nacional, na medida em que essa equiparação é suscetível de introduzir uma categoria intermédia entre a segurança nacional e a segurança pública, para efeitos da aplicação à segunda das exigências inerentes à primeira.

Em contrapartida, a Diretiva 2002/58, lida à luz da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado. Acrescenta que tal medida de conservação dirigida a locais ou infraestruturas regularmente frequentados por um número muito elevado de pessoas ou a locais estratégicos, como aeroportos, estações, portos marítimos ou zonas de portagens, é suscetível de permitir às autoridades competentes obter dados sobre a presença, nesses locais ou zonas geográficas para efeitos de luta contra a criminalidade grave, das pessoas que aí utilizam um meio de comunicação eletrónica e daí retirar, para efeitos da luta contra a criminalidade grave, conclusões sobre a sua presença e a sua atividade nos referidos locais ou zonas geográficas. Em todo o caso, a eventual existência de dificuldades para definir com precisão as hipóteses e as condições em que pode ser efetuada uma conservação seletiva não pode justificar que os Estados-Membros prevejam uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização.

Esta diretiva, lida à luz da Carta, também não se opõe a medidas legislativas que prevejam, para os mesmos fins, uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporal limitado ao estritamente necessário, bem como dos dados relativos à identidade civil dos utilizadores de comunicações eletrónicas. No que respeita a este último aspeto, o Tribunal de Justiça precisa, mais especificamente, que nem a Diretiva 2002/58 nem nenhum outro ato do direito da União se opõem a uma legislação nacional que tenha por objeto a luta contra a criminalidade grave, nos termos da qual a aquisição de um meio de comunicação eletrónica, como um cartão SIM pré-pago, esteja sujeita à verificação de documentos oficiais que comprovem a identidade do comprador e ao

[53] Consagrados nos artigos 7.° a 11.° da Carta.

registo, pelo vendedor, das informações daí resultantes, sendo o vendedor obrigado, se for caso disso, a dar acesso a essas informações às autoridades nacionais competentes.

O mesmo não se aplica às medidas legislativas que prevejam, ainda para efeitos da luta contra a criminalidade grave e da prevenção das ameaças graves contra a segurança pública, uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida («quick freeze») dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem. Com efeito, só a luta contra a criminalidade grave e, *a fortiori*, a salvaguarda da segurança nacional são suscetíveis de justificar essa conservação, desde que essa medida e o acesso aos dados conservados respeitem os limites do estritamente necessário. O Tribunal de Justiça recorda que essa medida de conservação rápida pode ser alargada aos dados de tráfego e aos dados de localização relativos a pessoas diferentes das que são suspeitas de ter planeado ou cometido uma infração penal grave ou uma ofensa à segurança nacional, desde que tais dados possam, com base em elementos objetivos e não discriminatórios, contribuir para o esclarecimento dessa infração ou dessa ofensa à segurança nacional, tais como os dados da vítima desta e do seu meio social ou profissional.

No entanto, o Tribunal de Justiça indica, em seguida, que todas as medidas legislativas acima mencionadas devem assegurar, mediante regras claras e precisas, que a conservação dos dados em causa esteja sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso. As diferentes medidas de conservação dos dados de tráfego e dos dados de localização podem, segundo a escolha do legislador nacional, e respeitando os limites do estritamente necessário, ser aplicadas conjuntamente.

Além disso, o Tribunal de Justiça precisa que autorizar, para efeitos da luta contra a criminalidade grave, um acesso a tais dados conservados de maneira generalizada e indiferenciada, para fazer face a uma ameaça grave para a segurança nacional, iria contra a hierarquia dos objetivos de interesse geral que podem justificar uma medida adotada ao abrigo da Diretiva 2002/58. Com efeito, isso equivaleria a permitir que o acesso pudesse ser justificado por um objetivo de importância menor do que aquele que justificou a conservação, a saber a salvaguarda da segurança nacional, correndo assim o risco de privar de qualquer efeito útil a proibição de proceder a uma conservação generalizada e indiferenciada para efeitos de luta contra a criminalidade grave.

Em segundo lugar, o Tribunal de Justiça decide que a Diretiva 2002/58, lida à luz da Carta, se opõe a uma legislação nacional, ao abrigo da qual o tratamento centralizado dos pedidos de acesso a dados conservados pelos prestadores de serviços de comunicações eletrónicas, que emanam da polícia no âmbito da investigação e da repressão de infrações penais graves, incumbe a um agente de polícia, mesmo quando este seja assistido por uma unidade instituída no âmbito da polícia que goza de um

certo grau de autonomia no exercício da sua missão e cujas decisões podem ser posteriormente objeto de fiscalização jurisdicional. Com efeito, por um lado, esse funcionário não cumpre as exigências de independência e de imparcialidade que se impõem a uma autoridade administrativa que exerce o controlo prévio dos pedidos de acesso aos dados emanados das autoridades nacionais competentes, na medida em que não tem a qualidade de terceiro em relação a essas autoridades. Por outro lado, embora a decisão desse funcionário possa ser objeto de fiscalização jurisdicional *ex post*, essa fiscalização não pode substituir uma fiscalização independente e, salvo em caso de urgência devidamente justificada, prévia.

Por último, em terceiro lugar, o Tribunal de Justiça confirma a sua jurisprudência segundo a qual o direito da União se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe, por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com a Diretiva 2002/58. Dito isto, o Tribunal de Justiça recorda que a admissibilidade dos meios de prova obtidos através dessa conservação cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade.

Acórdão de 20 de setembro de 2022 (Grande Secção), VD e SR (C-339/20 e C-397/20, EU:C:2022:703)

Na sequência de uma investigação conduzida pela Autorité des marchés financiers (Autoridade dos Mercados Financeiros, França, a seguir «AMF»), foram instaurados processos penais contra VD e SR, duas pessoas singulares acusadas de crimes de abuso de informação privilegiada, transmissão de informação privilegiada, cumplicidade, corrupção e branqueamento de capitais. No âmbito desta investigação, a AMF tinha utilizado dados pessoais decorrentes de chamadas telefónicas efetuadas por VD e SR, recolhidos com base no code des postes et des communications électroniques (Código dos Correios e das Comunicações Eletrónicas), no contexto da prestação de serviços de comunicações eletrónicas.

Na medida em que foram constituídos arguidos com base nos dados de tráfego disponibilizados pela AMF, VD e SR interpuseram, cada um, na cour d'appel de Paris (Tribunal de Recurso de Paris, França), um recurso, invocando, nomeadamente, um fundamento relativo à violação do artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.°, 11.° e 52.°, n.° 1, da Carta. Mais concretamente, baseando-se na

jurisprudência que resulta do Acórdão Tele2 Sverige e Watson e o [54]., VD e SR contestavam o facto de a AMF se ter baseado, para proceder à recolha dos referidos dados, nas disposições nacionais em causa, quando, na sua opinião, essas disposições, por um lado, não eram conformes com direito da União, uma vez que previam uma conservação generalizada e indiferenciada dos dados de ligação e, por outro, não previam nenhum limite ao poder dos inspetores da AMF de aceder aos dados conservados.

Com dois Acórdãos de 20 de setembro de 2018 e de 7 de março de 2019, a cour d'appel de Paris (Tribunal de Recurso de Paris) negou provimento aos recursos de VD e de SR. Para julgar improcedente o fundamento acima referido, os juízes que conheceram do mérito da causa basearam-se, nomeadamente, no facto de o Regulamento relativo ao abuso de mercado [55] permitir às autoridades competentes solicitar, na medida em que a legislação nacional o permita, os registos de dados de tráfego existentes na posse de um operador de serviços de comunicações eletrónicas, se houver motivos razoáveis para suspeitar de uma violação da proibição do abuso de informação privilegiada e que tais registos possam ser pertinentes para a investigação relativa a essa violação.

VD e SR interpuseram um recurso na Cour de cassation (Tribunal de Cassação, França), o órgão jurisdicional de reenvio nos presentes processos.

Neste contexto, esse órgão jurisdicional interroga-se sobre a conciliação entre o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz da Carta, e os requisitos que resultam do artigo 12.°, n.° 2, alíneas a) e d), da Diretiva «abuso de mercado» [56] e do artigo 23.°, n.° 2, alíneas g) e h), do Regulamento relativo ao abuso de mercado. Esta problemática tem origem nas medidas legislativas em causa no processo principal, que preveem a título preventivo, para efeitos da luta contra os crimes de abuso de mercado, de que fazem parte as operações de abuso de informações privilegiadas, para os operadores de serviços de comunicações eletrónicas, uma conservação generalizada e indiferenciada dos dados de tráfego, por um período de um ano a contar do dia do registo. No caso de o Tribunal de Justiça considerar que a legislação relativa à conservação dos dados de ligação, em causa no processo principal, não é conforme com o direito da União, coloca-se a questão da manutenção provisória dos efeitos dessa legislação, com vista a evitar uma situação de insegurança jurídica e permitir que os dados recolhidos e conservados anteriormente possam ser utilizados para efeitos de deteção e repressão das operações de abuso de informação privilegiada.

No seu acórdão, o Tribunal de Justiça, reunido em Grande Secção, declara que a conservação generalizada e indiferenciada dos dados de tráfego, por um período de um

54 Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970).

55 Regulamento (UE) n.° 596/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativo ao abuso de mercado (regulamento abuso de mercado) e que revoga a Diretiva 2003/6/CE do Parlamento Europeu e do Conselho e as Diretivas 2003/124/CE, 2003/125/CE e 2004/72/CE da Comissão (JO 2014, L 173, p. 1).

56 Diretiva 2003/6/CE do Parlamento Europeu e do Conselho, de 28 de janeiro de 2003, relativa ao abuso de informação privilegiada e à manipulação de mercado (abuso de mercado) (JO 2003, L 96, p. 16).

ano a contar do dia do registo, pelos operadores de serviços de comunicações eletrónicas não é autorizada, a título preventivo, para efeitos da luta contra os crimes de abuso de mercado. Além disso, confirma a sua jurisprudência segundo a qual o direito da União se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de ilegalidade que lhe incumbe, no que respeita a disposições legislativas nacionais incompatíveis com o direito da União.

O Tribunal de Justiça recorda, desde logo, que, para interpretar uma disposição do direito da União, há que ter em conta não só os seus termos mas também o seu contexto e os objetivos prosseguidos pela regulamentação de que faz parte.

No que se refere à redação das disposições referidas nas questões prejudiciais, há que constatar que, enquanto o artigo 12.°, n.° 2, alínea d), da Diretiva «abuso de mercado» se refere ao poder da AMF de «exigir a comunicação dos registos telefónicos e de transmissão de dados existentes», o artigo 23.°, n.° 2, alíneas g) e h), do Regulamento relativo ao abuso de mercado remete para o poder dessa autoridade de solicitar, por um lado, os «registos [...] de dados de tráfego na posse de empresas de investimento, instituições de crédito ou instituições financeiras» e, por outro, «na medida em que a legislação nacional o permita, os registos de tráfego de dados existentes na posse de um operador de telecomunicações». Segundo o Tribunal de Justiça, da redação destas disposições resulta inequivocamente que estas se limitam a enquadrar o poder da AMF de «exigir», ou ainda, de «solicitar» os dados na posse destes operadores, o que corresponde a um acesso a tais dados. Além disso, a referência feita aos registos «existentes», e «na posse» dos referidos operadores, dá a entender que o legislador da União não pretendeu regular a possibilidade de o legislador nacional impor uma obrigação de conservação de tais registos. Segundo o Tribunal de Justiça, esta interpretação é, por outro lado, corroborada tanto pelo contexto em que se inserem as referidas disposições como pelos objetivos prosseguidos pela regulamentação de que essas disposições fazem parte.

No que se refere ao contexto em que se inserem as disposições referidas pelas questões prejudiciais, o Tribunal de Justiça observa que, embora, nos termos das disposições relevantes da Diretiva «abuso de mercado» e do Regulamento relativo ao abuso de mercado [57], o legislador da União tenha pretendido impor aos Estados-Membros que adotassem as medidas necessárias para que as autoridades competentes em matéria financeira dispusessem de um conjunto de ferramentas, de competências e de recursos adequados, bem como de poderes de vigilância e de investigação necessários para assegurar a eficácia das suas missões, estas disposições nada referem quanto à eventual possibilidade de os Estados-Membros imporem, para o mesmo efeito, aos operadores de serviços de comunicações eletrónicas, uma obrigação de conservação generalizada e indiferenciada dos dados de tráfego, nem quanto às

[57] Respetivamente, Artigo 12.°, n.° 1, da Diretiva «abuso de mercado» e artigo 23.°, n.° 3, do Regulamento relativo ao abuso de mercado, lido à luz do considerando 62 deste regulamento.

condições em que esses dados devem ser conservados pelos referidos operadores com o objetivo de os comunicar, se for caso disso, às autoridades competentes.

No que se refere aos objetivos prosseguidos pela regulamentação em causa, o Tribunal de Justiça salienta que resulta, por um lado, da Diretiva «abuso de mercado» e, por outro, do Regulamento relativo ao abuso de mercado [58], que estes instrumentos têm por finalidade assegurar a integridade dos mercados financeiros na União e promover a confiança dos investidores nesses mercados, confiança essa que se baseia, nomeadamente, no facto de se encontrarem em pé de igualdade e protegidos da utilização ilícita de informação privilegiada. A proibição de operações de abuso de informação privilegiada enunciada nos referidos instrumentos [59] visa, assim, garantir a igualdade entre os contratantes numa transação bolsista, evitando que um deles, que possui uma informação privilegiada e se encontra, por esse facto, numa posição vantajosa relativamente aos outros investidores, seja beneficiado em detrimento dos que a desconhecem. Embora, nos termos do Regulamento relativo ao abuso de mercado [60], os registos dos dados de ligação constituam um elemento de prova crucial, por vezes única, para detetar e atestar a existência de um abuso de informação privilegiada ou de manipulação de mercado, não deixa de ser verdade que este regulamento apenas se refere aos registos «na posse de» operadores de serviços de comunicações eletrónicas, bem como ao poder da autoridade competente em matéria financeira de «solicitar» a comunicação dos dados «existentes» a esses operadores. Assim, não resulta de forma alguma da sua letra que o legislador da União tenha pretendido, com isto, conceder aos Estados-Membros o poder de impor aos operadores de serviços de comunicações eletrónicas uma obrigação geral de conservação de dados. Daqui resulta que nem a Diretiva «abuso de mercado» nem o Regulamento relativo ao abuso de mercado, são suscetíveis de constituir um fundamento jurídico de uma obrigação geral de conservação dos registos de dados de tráfego na posse dos operadores de serviços de comunicações eletrónicas para efeitos do exercício dos poderes conferidos à autoridade competente em matéria financeira ao abrigo destes atos.

Em seguida o Tribunal de Justiça recorda que a Diretiva 2002/58 constitui o ato de referência em matéria de conservação e, de maneira mais generalizada, de tratamento de dados pessoais no setor das comunicações eletrónicas, pelo que a sua interpretação, feita à luz desta diretiva, regula igualmente os registos dos dados de tráfego na posse dos operadores de serviços de comunicações eletrónicas, que as autoridades competentes em matéria financeira podem solicitar ao abrigo da Diretiva «abuso de mercado» e do Regulamento relativo ao abuso de mercado [61]. A apreciação da licitude

---

58 Respetivamente, considerandos 2 e 12 da Diretiva «abuso de mercado» e artigo 1.° do Regulamento relativo ao abuso de mercado, lido à luz dos considerandos 2 e 24 deste regulamento

59 Artigo 2.°, n.° 1, da Diretiva «abuso de mercado» e artigo 8.°, n.° 1, do Regulamento relativo ao abuso de mercado.

60 Considerando 62 do Regulamento relativo ao abuso de mercado.

61 Respetivamente, artigo 11.° da Diretiva «abuso de mercado» e artigo 22.° do Regulamento relativo ao abuso de mercado.

do tratamento dos registos na posse dos operadores de serviços de comunicações eletrónicas [62] deve, por conseguinte, ser efetuada à luz das condições previstas na Diretiva 2002/58, bem como da interpretação desta diretiva na jurisprudência do Tribunal de Justiça.

Assim, o Tribunal de Justiça considera que a Diretiva «abuso de mercado» e o Regulamento relativo ao abuso de mercado, lidos em conjugação com a Diretiva 2002/58 e à luz da Carta, se opõem a medidas legislativas que preveem, a título preventivo, para efeitos da luta contra os crimes de abuso de mercado, de que fazem parte as operações de abuso de informação privilegiada, uma conservação temporária dos dados de tráfego, a saber, por um período de um ano a contar do dia do registo, mas generalizada e indiferenciada, pelos operadores de serviços de comunicações eletrónicas.

Por último, o Tribunal de Justiça confirma a sua jurisprudência, segundo a qual o direito da União se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de ilegalidade que lhe incumbe, nos termos do direito nacional, relativamente a disposições legislativas nacionais que, por um lado, impõem aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego, e por outro, permitem a comunicação de tais dados à autoridade competente em matéria financeira, sem autorização prévia de um órgão jurisdicional ou de uma autoridade administrativa independente, devido à incompatibilidade dessas disposições com a Diretiva 2002/58, lida à luz da Carta. No entanto, o Tribunal de Justiça recorda que a admissibilidade dos meios de prova obtidos através dessa conservação cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao direito nacional, sem prejuízo do respeito, nomeadamente, dos princípios da equivalência e da efetividade. Este último princípio obriga o juiz penal nacional a afastar informações e elementos de prova obtidos através de uma conservação generalizada e indiferenciada incompatível com o direito da União se as pessoas em causa não estiverem em condições de contestar eficazmente essas informações e elementos de prova, provenientes de um domínio que escapa ao conhecimento dos juízes e que são suscetíveis de influenciar de modo preponderante a apreciação dos factos.

Acórdão de 30 de abril de 2024 (Tribunal Pleno), La Quadrature du Net e o. (Dados pesoais e luta contra a contrafação) (C-470/21, EU:C:2024:370)

Questionado, a título prejudicial, pelo Conseil d'État (Conselho de Estado, em formação jurisdicional, França), o Tribunal Pleno do Tribunal de Justiça desenvolve a sua jurisprudência sobre a Diretiva 2002/58, fornecendo precisões relativas, por um lado, às

[62] Na aceção do artigo 12.°, n.° 2, alínea b), da Diretiva «abuso de mercado» e artigo 23.°, n.° 2, alíneas g) e h), do Regulamento relativo ao abuso de mercado.

condições em que uma conservação generalizada de endereços IP por prestadores de serviços de comunicações eletrónicas pode não ser considerada constitutiva de uma ingerência grave nos direitos ao respeito da vida privada, à proteção dos dados pessoais e à liberdade de expressão garantidos pela Carta [63], bem como, por outro, à possibilidade de uma autoridade pública aceder a certos dados pessoais conservados no respeito de tais condições, no âmbito da luta contra as infrações aos direitos de propriedade intelectual cometidas em linha.

No caso em apreço, quatro associações apresentaram ao Premier ministre (Primeiro-Ministro, França) um pedido de revogação do Decreto relativo ao tratamento automatizado de dados pessoais [64]. Não tendo sido dado seguimento a este pedido, estas associações interpuseram no Conseil d'État um recurso de anulação dessa decisão tácita de indeferimento. Alegaram que este decreto e as disposições que constituem a sua base jurídica [65] violam o direito da União.

Ao abrigo da legislação francesa, a Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [Alta Autoridade para a Divulgação das Obras e a Proteção dos Direitos na Internet (Hadopi)], para poder identificar os responsáveis pelas violações dos direitos de autor ou dos direitos conexos cometidas em linha, está autorizada a aceder a certos dados que os prestadores de serviços de comunicações eletrónicas devem conservar. Estes dados incidem sobre a identidade civil da pessoa em causa e correspondem ao seu endereço IP recolhido previamente por organismos de titulares de direitos. Uma vez identificado o titular do endereço IP utilizado em atividades que violam esses direitos, a Hadopi segue o procedimento designado «resposta graduada». Em concreto, é competente para enviar, a essa pessoa, duas recomendações que se assemelham a advertências e, se as atividades persistirem, uma carta que a notifica de que as suas atividades são passíveis de ação penal. Por último, tem o direito de submeter a questão ao Ministério Público com vista a procedimento penal contra a referida pessoa [66].

Neste contexto, o Conseil d'État questionou o Tribunal de Justiça sobre a interpretação da Diretiva 2002/58, lida à luz da Carta [67].

---

63 Artigos 7.°, 8.° e 11.° da Carta.

64 Décret n.° 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé «Système de gestion des mesures pour la protection des œuvres sur internet» (Decreto n.° 2010-236, de 5 de março de 2010, relativo ao tratamento automatizado de dados pessoais autorizado pelo artigo L-331-29 do Código da Propriedade Intelectual designado «Sistema de gestão das medidas de proteção das obras na Internet») (JORF n.° 56 de 7 de março de 2010, texto n.° 19), conforme alterado pelo Décret n.° 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (Decreto n.° 2017-924, de 6 de maio de 2017, relativo à gestão dos direitos de autor e dos direitos conexos por um organismo de gestão de direitos e que altera o Código da Propriedade Intelectual) (JORF n.° 109 de 10 de maio de 2017, texto n.° 176).

65 Nomeadamente o artigo L. 331-21, terceiro a quinto parágrafos, do Código da Propriedade Intelectual.

66 A partir de 1 de janeiro de 2022, a Hadopi fundiu-se com o Conseil supérieur de l'audiovisuel (Conselho Superior do Audiovisual, CSA), outra autoridade pública independente, para constituir a Autorité de régulation de la communication audiovisuelle et numérique (Autoridade Reguladora da Comunicação Audiovisual e Digital, ARCOM). No entanto, o procedimento de resposta graduada manteve-se, em substância, inalterado.

67 Artigo 15.°, n.° 1, da Diretiva 2002/58.

Em primeiro lugar, no que respeita à conservação dos dados relativos à identidade civil e dos endereços IP correspondentes, o Tribunal de Justiça sublinha que nem toda a conservação generalizada e indiferenciada dos endereços IP constitui necessariamente uma ingerência grave nos direitos ao respeito da vida privada, à proteção dos dados pessoais e à liberdade de expressão garantidos pela Carta.

A obrigação de assegurar tal conservação pode ser justificada pelo objetivo da luta contra as infrações penais em geral, quando se exclui efetivamente que esta conservação possa resultar em ingerências graves na vida privada da pessoa em causa devido à possibilidade de tirar conclusões precisas sobre esta, nomeadamente, ao associar esses endereços IP a um conjunto de dados de tráfego ou de localização.

Por conseguinte, um Estado-Membro que pretenda impor aos prestadores de serviços de comunicações eletrónicas esta obrigação deve assegurar-se de que as modalidades de conservação desses dados excluem que se possam tirar conclusões específicas sobre a vida privada das pessoas em causa.

O Tribunal de Justiça esclarece que as modalidades de conservação devem, para o efeito, ser referentes à própria estrutura da conservação que, em substância, deve ser organizada de modo a garantir uma separação efetivamente estanque das diferentes categorias de dados conservados. Assim, as disposições nacionais relativas a essas modalidades devem assegurar que cada categoria de dados, incluindo os dados relativos à identidade civil e os endereços IP, seja conservada de forma totalmente separada das outras categorias de dados conservados e que esta separação seja efetivamente estanque, através de um dispositivo informático seguro e fiável. Além disso, uma vez que preveem a possibilidade de associar os endereços IP conservados à identidade civil da pessoa em causa para efeitos de luta contra as infrações, estas disposições só devem permitir essa associação através da utilização de um processo técnico de desempenho elevado que não ponha em causa a eficácia da separação estanque das categorias de dados. A fiabilidade desta separação deve ser objeto de um controlo regular por uma autoridade pública terceira. Desde que a legislação nacional aplicável preveja tais exigências estritas, a ingerência resultante dessa conservação dos endereços IP não pode ser qualificada de «grave».

Por conseguinte, o Tribunal de Justiça conclui que, perante um dispositivo legislativo que garanta que nenhuma combinação de dados permitirá tirar conclusões precisas sobre a vida privada das pessoas cujos dados são conservados, a Diretiva 2002/58, lida à luz da Carta, não se opõe a que um Estado-Membro imponha uma obrigação de conservação generalizada e indiferenciada dos endereços IP, por um período que não ultrapasse o estritamente necessário, para efeitos de luta contra as infrações penais em geral.

Em segundo lugar, no que respeita ao acesso a dados relativos à identidade civil correspondentes a endereços IP, o Tribunal de Justiça declara que a Diretiva 2002/58, lida à luz da Carta, não se opõe, em princípio, a uma regulamentação nacional que permite o acesso, por uma autoridade pública, a esses dados conservados pelos

prestadores de serviços de comunicações eletrónicas de forma separada e efetivamente estanque, com o único objetivo de permitir a essa autoridade identificar os titulares desses endereços suspeitos de serem responsáveis por violações dos direitos de autor e dos direitos conexos na Internet e tomar medidas a seu respeito. Nesse caso, a regulamentação nacional deve proibir os agentes que dispõem desse acesso, primeiro, de divulgar sob qualquer forma informações sobre o conteúdo dos ficheiros consultados por esses titulares, exceto com o único objetivo de os remeter ao Ministério Público, segundo, de efetuar qualquer rastreio da navegação desses titulares e, terceiro, de utilizar esses endereços IP para fins diferentes da adoção dessas medidas.

Neste contexto, o Tribunal de Justiça recorda, nomeadamente, que, ainda que a liberdade de expressão e a confidencialidade dos dados pessoais sejam preocupações primordiais, estes direitos fundamentais não são, porém, absolutos. Com efeito, após uma ponderação dos direitos e interesses em causa, estes devem por vezes ceder perante outros direitos fundamentais e imperativos de interesse geral como a defesa da ordem pública e a prevenção das infrações penais ou a proteção dos direitos e liberdades de terceiros. É o que sucede, em especial, quando a preponderância concedida às referidas preocupações primordiais é suscetível de prejudicar a eficácia de um inquérito penal, nomeadamente, ao tornar impossíveis ou excessivamente difíceis a identificação efetiva do autor de uma infração penal e a aplicação de uma sanção.

Neste mesmo contexto, o Tribunal de Justiça faz referência igualmente à sua jurisprudência segundo a qual, no que respeita à luta contra as infrações penais que violam direitos de autor ou direitos conexos cometidas em linha, a circunstância de o acesso aos endereços IP poder constituir o único meio de investigação que permite a identificação da pessoa em causa tende a demonstrar que a conservação desses endereços e o acesso aos mesmos são estritamente necessários para alcançar o objetivo pretendido e respeitam, por isso, a exigência de proporcionalidade. Não permitir esse acesso comportaria, aliás, um risco real de impunidade sistémica de infrações penais cometidas em linha ou cuja prática ou preparação é facilitada pelas características próprias da Internet. Ora, a existência desse risco constitui uma circunstância pertinente para apreciar, no âmbito de uma ponderação dos diferentes direitos e interesses em causa, se uma ingerência nos direitos ao respeito da vida privada, à proteção dos dados pessoais e à liberdade de expressão é uma medida proporcionada à luz do objetivo de luta contra as infrações penais.

Em terceiro lugar, ao pronunciar-se sobre a questão de saber se o acesso da autoridade pública a dados relativos à identidade civil correspondentes a um endereço IP deve ser sujeito a um controlo prévio por um órgão jurisdicional ou por uma entidade administrativa independente, o Tribunal de Justiça considera que a exigência deste controlo se impõe quando, no contexto de uma regulamentação nacional, o acesso comporta o risco de uma ingerência grave nos direitos fundamentais da pessoa em causa no sentido de que poderia permitir a essa autoridade pública tirar conclusões precisas sobre a vida privada dessa pessoa e, se for caso disso, estabelecer o seu perfil

pormenorizado. Inversamente, esta exigência de um controlo prévio não é aplicável quando a ingerência nos direitos fundamentais não possa ser qualificada de grave.

A este respeito, o Tribunal de Justiça esclarece que, se for criado um dispositivo de conservação que garanta uma separação efetivamente estanque das diferentes categorias de dados conservados, o acesso da autoridade pública aos dados relativos à identidade civil correspondentes aos endereços IP não está, em princípio, sujeito à exigência de um controlo prévio. Com efeito, este acesso que tem por única finalidade identificar o titular de um endereço IP não constitui, regra geral, uma ingerência grave nos direitos acima referidos.

No entanto, o Tribunal de Justiça não exclui que, em situações atípicas, no âmbito de um procedimento como o procedimento de resposta graduada em causa no processo principal, exista o risco de a autoridade pública poder tirar conclusões precisas sobre a vida privada da pessoa em causa, nomeadamente, quando essa pessoa exerça atividades que violam direitos de autor ou direitos conexos, em redes descentralizadas (*peer-to-peer*), de forma reiterada ou em grande escala, relacionadas com obras protegidas de tipos específicos, revelando informações, eventualmente sensíveis, sobre a vida privada da referida pessoa.

No caso em apreço, um titular de um endereço IP pode estar particularmente exposto a esse risco quando a autoridade pública é chamada a decidir se deve ou não submeter a questão ao Ministério Público com vista a procedimento penal. Com efeito, a intensidade da violação do direito ao respeito da vida privada é suscetível de aumentar à medida que o procedimento de resposta graduada, que opera segundo um processo sequencial, percorre as diferentes fases que o compõem. O acesso da autoridade competente a todos os dados relativos à pessoa em causa e acumulados durante as diferentes fases desse procedimento pode permitir tirar conclusões precisas sobre a sua vida privada. Por conseguinte, a regulamentação nacional deve prever um controlo prévio que deve ocorrer antes de a autoridade pública poder associar dados relativos à identidade civil a esse conjunto de dados, e antes do eventual envio da notificação da prática por essa pessoa de factos suscetíveis de ação penal. Este controlo deve, por outro lado, preservar a eficácia do procedimento de resposta graduada, permitindo, em especial, identificar os casos de possível reiteração do comportamento infrator em causa. Para o efeito, este procedimento deve ser organizado e estruturado de forma a que os dados de identidade civil de uma pessoa correspondentes a endereços IP previamente recolhidos na Internet não sejam automaticamente suscetíveis de ser associados, pelas pessoas responsáveis pela apreciação dos factos na autoridade pública competente, a elementos de que esta última já dispõe e que possam permitir tirar conclusões precisas sobre a vida privada dessa pessoa.

Além disso, no que respeita ao objeto do controlo prévio, o Tribunal de Justiça salienta que, nos casos em que a pessoa em causa é suspeita de ter cometido uma infração abrangida pelas infrações penais em geral, o órgão jurisdicional ou a entidade administrativa independente responsável por este controlo deve recusar o acesso

quando este último permita à autoridade pública tirar conclusões precisas sobre a vida privada da referida pessoa. Em contrapartida, mesmo um acesso que permita tirar tais conclusões precisas deve ser autorizado nos casos em que a pessoa em causa seja suspeita de ter cometido crimes que o Estado-Membro em causa considera que violam um interesse fundamental da sociedade e que são, assim, abrangidos pelo âmbito da criminalidade grave.

O Tribunal de Justiça esclarece igualmente que o controlo prévio nunca pode ser totalmente automatizado, uma vez que, no âmbito de um inquérito penal, este controlo exige a ponderação, por um lado, dos interesses legítimos ligados à luta contra a criminalidade e, por outro, do respeito da vida privada e da proteção dos dados pessoais. Esta ponderação necessita da intervenção de uma pessoa singular, sendo esta tanto mais necessária quanto o automatismo e a grande escala do tratamento de dados em causa implicam riscos para a vida privada.

Assim, o Tribunal de Justiça conclui que a possibilidade de as pessoas responsáveis pela apreciação dos factos na autoridade pública associarem dados relativos à identidade civil de uma pessoa correspondentes a um endereço IP a ficheiros que contêm elementos que permitam conhecer o título de obras protegidas cuja disponibilização na Internet justificou a recolha dos endereços IP por organismos de titulares de direitos deve estar sujeita, nos casos de repetição pela mesma pessoa de uma atividade que viola direitos de autor ou direitos conexos, a um controlo por um órgão jurisdicional ou por uma entidade administrativa independente. Este controlo não pode ser totalmente automatizado e deve ocorrer previamente a essa associação, suscetível, nesses casos, de permitir que sejam tiradas conclusões precisas sobre a vida privada da referida pessoa cujo endereço IP foi utilizado para atividades que podem violar direitos de autor ou direitos conexos.

Em quarto e último lugar, o Tribunal Justiça declara que o sistema de tratamento de dados utilizado pela autoridade pública deve ser regularmente objeto de um controlo por um organismo independente e com a qualidade de terceiro em relação a essa autoridade pública. Este controlo visa verificar a integridade do sistema, incluindo as garantias efetivas contra os riscos de acesso e utilização abusivos ou ilícitos desses dados, bem como a sua eficácia e fiabilidade para detetar eventuais incumprimentos.

Neste contexto, o Tribunal de Justiça observa que, no caso em apreço, o tratamento automatizado dos dados pessoais efetuado pela autoridade pública com base nas informações relativas às contrafações constatadas pelos organismos de titulares de direitos é suscetível de comportar um certo número de falsos casos positivos e, sobretudo, o risco de um número de dados potencialmente muito elevado ser desviado por terceiros para fins abusivos ou ilícitos, o que explica a necessidade desse controlo. Além disso, acrescenta que este tratamento deve respeitar as regras específicas de proteção dos dados pessoais previstas pela Diretiva 2016/680. Com efeito, no caso em apreço, ainda que a autoridade pública não disponha de poderes decisórios próprios no âmbito do procedimento designado resposta graduada, deve ser qualificada de

«autoridade pública» envolvida na prevenção e deteção de infrações penais, e está, por conseguinte, abrangida pelo seu âmbito de aplicação. Assim, as pessoas envolvidas nesse procedimento devem beneficiar de um conjunto de garantias materiais e processuais estabelecido pela Diretiva 2016/680, cabendo ao órgão jurisdicional de reenvio verificar se estas garantias estão previstas na legislação nacional.

2. Tratamento de dados pessoais em matéria penal

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 [68] 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,

[68] 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 (JO 2000, L 239, p. 19, a seguir «CAAS»).

o tratamento dos seus dados pessoais, que figuram no alerta vermelho, é contrário à Diretiva 2016/680, relativa à proteção dos dados pessoais em matéria penal [69].

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 de Justiça 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 nesta diretiva.

No que diz respeito à questão relativa aos dados pessoais que figuram num alerta vermelho da Interpol, o Tribunal de Justiça 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 [70]. 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 [71]. 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.

Nestas condições, o Tribunal de Justiça 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

---

69 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).

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

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

efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais [72].

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 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*.

Acórdão de 21 de junho de 2022 (Grande Secção), Ligue des droits humains (C-817/19, EU:C:2022:491)

Neste processo (v. igualmente rubrica I.1., intitulada «Conformidade do direito derivado da União com o direito à proteção de dados pessoais», após ter declarado a validade da Diretiva PNR, o Tribunal de Justiça fornece esclarecimentos quanto à interpretação de algumas disposições desta diretiva [73].

Em primeiro lugar, o Tribunal de Justiça salienta que a diretiva enumera exaustivamente os objetivos prosseguidos pelo tratamento dos dados PNR. Por conseguinte, esta diretiva opõe-se a uma legislação nacional que autoriza o tratamento de dados PNR para fins diferentes da luta contra as infrações terroristas e a criminalidade grave. Assim, uma legislação nacional que admite, além disso, como finalidade do tratamento dos dados PNR, o acompanhamento das atividades visadas pelos serviços de informação e de segurança é suscetível de violar o caráter exaustivo dessa enumeração. Do mesmo modo, o sistema instituído pela Diretiva PNR não pode ser previsto para efeitos da melhoria dos controlos nas fronteiras e da luta contra a imigração clandestina. Daqui resulta igualmente que os dados PNR não podem ser conservados numa única base de dados que possa ser consultada com vista à prossecução tanto das finalidades da Diretiva PNR como de outras finalidades.

Em segundo lugar, o Tribunal de Justiça explicita o conceito de autoridade nacional independente, competente para analisar se os requisitos de comunicação dos dados PNR, para efeitos da sua avaliação posterior, estão preenchidos e para aprovar essa comunicação. Em especial, a autoridade criada como UIP não pode ser qualificada como tal, uma vez que não tem a qualidade de terceiro em relação à autoridade que pede o acesso aos dados. Com efeito, uma vez que os membros do seu pessoal podem ser

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

[73] Em particular, artigo 2.° («Aplicação da [diretiva] aos voos intra UE»), artigo 6.° («Tratamento dos dados PNR»), e artigo 12.° («Prazo de conservação e anonimização dos dados»), da Diretiva PNR.

agentes destacados pelas autoridades habilitadas a pedir esse acesso, a UIP surge necessariamente ligada a essas autoridades. Por conseguinte, a Diretiva PNR opõe-se a uma legislação nacional segundo a qual a autoridade criada como UIP tem igualmente a qualidade de autoridade nacional competente, habilitada a aprovar a comunicação dos dados PNR decorrido o prazo de seis meses subsequente à transferência desses dados para a UIP.

Em terceiro lugar, no que diz respeito ao prazo de conservação dos dados PNR, o Tribunal de Justiça declara que o artigo 12.° da Diretiva PNR, lido à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da Carta, se opõe a uma legislação nacional que prevê um prazo geral de conservação desses dados de cinco anos, aplicável indiferentemente a todos os passageiros aéreos.

Com efeito, segundo Tribunal de Justiça, após o decurso do prazo de conservação inicial de seis meses, a conservação dos dados PNR não se afigura limitada ao estritamente necessário no que respeita aos passageiros aéreos relativamente aos quais, nem as eventuais verificações efetuadas durante o prazo de conservação inicial de seis meses, nem qualquer outra circunstância, revelaram a existência de elementos objetivos — como o facto de os dados PNR dos passageiros em causa terem dado lugar a uma concordância positiva verificada no âmbito da avaliação prévia — suscetíveis estabelecer um risco em matéria de infrações terroristas ou de criminalidade grave que apresentem um nexo objetivo, pelo menos indireto, com a viagem aérea efetuada por esses passageiros. Em contrapartida, considera que, durante o período inicial de seis meses, a conservação dos dados PNR de todos os passageiros aéreos sujeitos ao sistema instituído por essa diretiva não parece, em princípio, exceder os limites do estritamente necessário.

Em quarto lugar, o Tribunal de Justiça fornece indicações relativas a uma eventual aplicação da Diretiva PNR, para efeitos da luta contra as infrações terroristas e a criminalidade grave, a outros modos de transporte que encaminhem passageiros para a União. Ora, a diretiva, lida à luz do artigo 3.°, n.° 2, TUE, do artigo 67.°, n.° 2, TFUE e do artigo 45.° da Carta, opõe-se a um sistema de transferência e de tratamento dos dados PNR de todos os transportes efetuados por outros meios no interior da União, se o Estado-Membro em causa não estiver perante uma ameaça terrorista real e atual ou previsível. Com efeito, nessa situação, como no caso dos voos intra-UE, a aplicação do sistema estabelecido pela Diretiva PNR deve limitar-se aos dados PNR dos transportes relativos, nomeadamente, a certas ligações ou a certos planos de viagem ou ainda a certas gares ou portos marítimos, relativamente aos quais existem indicações suscetíveis de justificar essa aplicação. Compete ao Estado-Membro em causa selecionar os transportes para os quais tais indicações existem e reexaminar regularmente essa aplicação em função da evolução das condições que justificaram a sua seleção.

IV. Transferência de dados pessoais para países terceiros

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

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 95/46.

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.

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 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.

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

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 [74], a Comissão ter considerado que, no contexto do regime

[74] 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).

denominado «porto seguro» (em inglês «safe harbour») [75], os Estados Unidos asseguravam um nível de proteção adequado aos dados pessoais transferidos.

Foi neste contexto que o Tribunal de Justiça 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, 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 referido artigo 25.°, n.° 6, da Diretiva 95/46.

O Tribunal de Justiça 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. Acresce que, 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.

Além disso, o Tribunal de Justiça 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. O Tribunal de Justiça concluiu que a invalidade dos artigos 1.° e 3.° da Decisão 2000/520 tinha por efeito afetar a validade desta decisão na sua totalidade.

No que respeita à impossibilidade de justificar tal ingerência, o Tribunal de Justiça 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

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

mínimo de exigências, de modo 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.

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. 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. 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.

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 de Justiça pronunciou-se pela primeira vez sobre a compatibilidade de um projeto de acordo internacional com a Carta, em particular com as disposições relativas ao respeito pela vida privada e à proteção de 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 de Justiça para saber se o projeto de acordo era conforme com o direito da União.

O projeto de acordo permite a transferência sistemática e contínua dos dados PNR de todos os passageiros para uma autoridade canadiana com vista à sua utilização e armazenamento, bem como a eventual transferência ulterior desses dados para outras autoridades e outros países terceiros, com objetivo de 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 impõe 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 projeto de acordo 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 de Justiça 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 de Justiça 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 de dados pessoais garantido pelo artigo 8.° da Carta, visto que constituem tratamentos de dados pessoais.

Além disso, o Tribunal de Justiça 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 projeto de acordo (informações que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas, etc.).

A este respeito, o Tribunal de Justiça 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 de Justiça 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 de Justiça 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.

Em segundo lugar, o Tribunal de Justiça 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, podem apresentar um risco em termos de luta contra o terrorismo e a criminalidade transnacional grave é admissível depois de terminada a sua estada nesse país, mesmo por um período de cinco anos.

Em terceiro lugar, o Tribunal de Justiça declarou que o direito fundamental ao respeito pela vida privada, consagrado no artigo 7.° da Carta, implica que a pessoa em causa se possa certificar 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 tratamento.

A este respeito, o Tribunal de Justiça 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.

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

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 este 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 [76]. 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 [77]. 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 [78].

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 [79], tinha constatado que os Estados Unidos asseguravam um nível de proteção adequado. Por Acórdão proferido em 6 de outubro de 2015, o Tribunal de Justiça, chamado a pronunciar-se sobre uma questão prejudicial submetida pela High Court (Tribunal Superior, Irlanda), declarou esta decisão inválida (a seguir «Acórdão Schrems I») [80].

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 de Justiça. 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

76 Artigo 45.º do RGPD.
77 Artigo 46.º, n.os 1 e 2, alínea c), do RGPD.
78 Artigo 49.º do RGPD.
79 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).
80 Acórdão do Tribunal de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650.

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 [81]. 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 High Court com vista a que esta submetesse um pedido de decisão prejudicial ao Tribunal de Justiça. 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 [82].

Através do seu pedido de decisão prejudicial, o órgão jurisdicional de reenvio interroga o Tribunal de Justiça 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 de Justiça constata que a análise da Decisão 2010/87 à luz da Carta não revela nenhum elemento suscetível de afetar a sua validade. Em contrapartida, o Tribunal de Justiça declarou a Decisão 2016/1250 inválida.

O Tribunal de Justiça 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 de Justiça 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.

No que diz respeito ao nível de proteção exigido no contexto de tal transferência, o Tribunal de Justiça 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 de Justiça

[81] 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).

[82] 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).

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.

Quanto às obrigações que incumbem às autoridades de controlo no contexto dessa transferência, o Tribunal de Justiça 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 caso de o exportador estabelecido na União não ter ele próprio suspendido ou posto termo a essa transferência.

Em seguida, o Tribunal de Justiça 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 de Justiça 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 de Justiça 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 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.

Por último, o Tribunal de Justiça 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 de Justiça observa que esta decisão, à semelhança da Decisão 2000/520, 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 de Justiça, 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 enquadradas 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 de Justiça 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 de Justiça 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.

Quanto à exigência de proteção jurisdicional, o Tribunal de Justiça 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 de Justiça declarou a Decisão 2016/1250 inválida.

V. Proteção de dados pessoais na Internet

1. Direito de oposição ao tratamento de 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 (v. igualmente rubricas II.1. e II.3., intituladas «Âmbito de aplicação da regulamentação geral» e «Conceito de "tratamento de dados pessoais"»), o Tribunal de Justiça 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 de Justiça 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, 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 de Justiça 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.

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 de Justiça 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. 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. 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.

Por último, o Tribunal de Justiça 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.

2. Tratamento de dados pessoais e direitos de propriedade intelectual

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

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 de Justiça 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 de Justiça, 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 de Justiça 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») [83], 2001/29/CE, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação [84], 2004/48/CE, relativa ao respeito dos direitos de propriedade intelectual [85], 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

[83] 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).

[84] 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).

[85] 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);

entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito comunitário, como o princípio da proporcionalidade.

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 de decisão prejudicial ao Tribunal de Justiça com vista à interpretação das Diretivas 2002/58 e 2004/48, no âmbito de um litígio que opõe a Bonnier Audio AB, a Earbooks AB, a Norstedts Förlagsgrupp AB, a 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 de Justiça 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 de Justiça 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 para 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.

A este respeito, o Tribunal de Justiça constatou 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.

Por conseguinte, o Tribunal de Justiça 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.

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*)

Neste acórdão, o Tribunal de Justiça, 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 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 (Conselho de Estado, em formação jurisdicional, França), chamado a pronunciar-se, pediu ao Tribunal de Justiça 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 de Justiça 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 [86], sob reserva de algumas exceções e derrogações. No que diz respeito ao tratamento de dados 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 [87].

O Tribunal de Justiça 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 de dados pessoais.

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.

Em segundo lugar, o Tribunal de Justiça 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 [88], 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 [89].

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 de Justiça sublinhou que, embora os direitos ao respeito da vida privada e à proteção de dados

86 Artigo 8, n.º 1, da Diretiva 95/46/CE e artigo 9.º, n.º 1, do Regulamento 2016/679.
87 Artigo 8.º, n.º 5, da Diretiva 95/46/CE e artigo 10.º do Regulamento 2016/679.
88 Artigo 8.º, n.º 2, alínea e), da Diretiva 95/46/CE e artigo 9.º, n.º 2, alínea e) do Regulamento 2016/679.
89 Artigo 14.º, primeiro parágrafo, alínea a), da Diretiva 95/46/CE e artigo 21.º, n.º 1, do Regulamento 2016/679.

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.

Em terceiro lugar, o Tribunal de Justiça 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, 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.

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

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 do 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 (Conselho de Estado, em formação jurisdicional, França), chamado a conhecer do processo pela Google, pediu que o Tribunal de Justiça precisasse qual o alcance territorial da obrigação de um operador de um motor de busca aplicar o direito à supressão de referências em aplicação da Diretiva 95/46.

O Tribunal de Justiça 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 [90].

No que respeita ao alcance do direito à supressão de referências, o Tribunal de Justiça 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 [91] que, para a realização desse objetivo, o legislador tenha optado por atribuir ao direito à 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 em 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.

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.

Por último, o Tribunal de Justiça 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

[90] Artigo 4.°, n.° 1, alínea a), da Diretiva 95/46/CE, e artigo 3.°, n.° 1, do Regulamento 2016/679.

[91] Artigos 12.°, alínea b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46/CE, e artigo 17.°, n.° 1, do Regulamento 2016/679.

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.

Acórdão de 8 de dezembro de 2022 (Grande Secção), Google (Supressão de um conteúdo pretensamente inexato) (C-460/20, EU:C:2022:962)

Os recorrentes no processo principal, TU, que ocupa cargos de responsabilidade e detém participações em diferentes sociedades, e RE, que era a sua companheira e, até maio de 2015, mandatária de uma dessas sociedades, foram objeto de três artigos publicados num sítio Internet em 2015 pela G LLC, operadora desse sítio Internet. Esses artigos, um dos quais ilustrado com quatro fotografias representando os recorrentes e que sugeriam que estes últimos levavam uma vida luxuosa, apresentavam de maneira crítica o modelo de investimento de várias das suas sociedades. O acesso a esses artigos era possível, no motor de busca explorado pela Google LLC (a seguir «Google»), através dos apelidos e nomes próprios dos recorrentes, tanto isoladamente como em conjugação com determinados nomes de sociedades. A lista de resultados remetia para esses artigos através de uma hiperligação, bem como para as fotografias exibidas sob a forma de imagens de prévisualização («*thumbnails*»).

Os recorrentes no processo principal solicitaram à Google, enquanto responsável pelo tratamento de dados pessoais efetuado pelo seu motor de busca, por um lado, que suprimisse da lista dos resultados de pesquisa as hiperligações para os artigos em causa, por conterem alegações inexatas e opiniões difamatórias, e, por outro, que retirasse as imagens de pré-visualização da lista dos resultados de pesquisa. A Google recusou dar seguimento a esse pedido.

Tendo sido vencidos tanto em primeira instância como no recurso, os recorrentes no processo principal interpuseram recurso de «Revision» para o Bundesgerichtshof (Supremo Tribunal de Justiça Federal, Alemanha), no âmbito do qual o Bundesgerichtshof submeteu ao Tribunal de Justiça um pedido de decisão prejudicial quanto à interpretação do RGPD e da Diretiva 95/46 [92].

No seu acórdão, proferido pela Grande Secção, o Tribunal de Justiça desenvolve a sua jurisprudência sobre as condições aplicáveis aos pedidos de supressão de referências dirigidos ao operador de um motor de busca com base nas regras relativas à proteção de dados pessoais. Em particular, examina, por um lado, o alcance das obrigações e responsabilidades que incumbem ao operador de um motor de busca no tratamento de

[92] Respetivamente, artigo 17.°, n.° 3, alínea a), do RGPD e artigo 12.°, alínea b), e artigo 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46.

um pedido de supressão de referências baseado na pretensa inexatidão das informações que figuram no conteúdo apresentado e, por outro, o ónus da prova imposto à pessoa em causa no que respeita a essa inexatidão. Além disso, pronuncia-se sobre a necessidade, para efeitos da apreciação de um pedido de supressão de fotografias exibidas sob a forma de imagens de pré-visualização na lista de resultados de uma pesquisa de imagens, de ter em conta o contexto inicial da publicação dessas fotografias na Internet.

Em primeiro lugar, o Tribunal de Justiça declarou que, no âmbito da ponderação entre, por um lado, os direitos ao respeito pela vida privada e à proteção dos dados pessoais, e, por outro, o direito à liberdade de expressão e de informação [93], para efeitos da apreciação de um pedido de supressão de referências dirigido ao operador de um motor de busca e destinado a suprimir da lista de resultados de uma pesquisa a hiperligação para um conteúdo que contém informações pretensamente inexatas, essa supressão de referências não está sujeita à condição de a questão da exatidão do conteúdo apresentado ter sido resolvida, pelo menos provisoriamente, no âmbito de uma ação intentada pelo requerente contra o fornecedor de conteúdos.

A título preliminar, para examinar em que condições o operador de um motor de busca está obrigado a deferir um pedido de supressão de referências e assim a suprimir da lista de resultados, exibida após uma pesquisa efetuada a partir do nome da pessoa em causa, a hiperligação para uma página Internet, na qual figuram alegações que essa pessoa considera inexatas, o Tribunal de Justiça recordou nomeadamente o seguinte:

• na medida em que a atividade de um motor de busca é suscetível de afetar, significativamente e por acréscimo à dos editores de sítios Internet, os direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais, o operador desse motor, como pessoa que determina as finalidades e os meios dessa atividade, deve assegurar, no âmbito das suas responsabilidades, das suas competências e das suas possibilidades, que as garantias previstas na Diretiva 95/46 e no RGPD possam produzir pleno efeito e possa efetivamente realizar-se uma proteção eficaz e completa das pessoas em causa;

• o operador de um motor de busca, perante um pedido de supressão de referências, deve verificar se a inclusão da hiperligação para a página Internet em questão na lista de resultados é necessária ao exercício do direito à liberdade de informação dos internautas potencialmente interessados em aceder a essa página Internet através dessa pesquisa, protegida pelo direito à liberdade de expressão e de informação;

• o RGPD consagra expressamente a exigência de uma ponderação entre, por um lado, os direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais e, por outro, o direito fundamental à liberdade de informação.

[93] Direitos fundamentais garantidos respetivamente pelos artigos 7.°, 8.° e 11.° da Carta.

Antes de mais, o Tribunal de Justiça salienta que, embora, regra geral, os direitos da pessoa em causa ao respeito pela vida privada e à proteção de dados pessoais prevaleçam sobre o interesse legítimo dos internautas em aceder à informação em questão, este equilíbrio pode, todavia, depender das circunstâncias pertinentes de cada caso, nomeadamente da natureza dessa informação e da sua sensibilidade para a vida privada da pessoa em causa, bem como do interesse do público em dispor da referida informação, o qual pode variar, designadamente, em função do papel desempenhado por essa pessoa na vida pública.

A questão do caráter exato ou não do conteúdo apresentado constitui igualmente um elemento pertinente no âmbito dessa apreciação. Assim, em certas circunstâncias, o direito à informação dos internautas e a liberdade de expressão do fornecedor de conteúdos podem prevalecer sobre os direitos à proteção da vida privada e à proteção dos dados pessoais, nomeadamente quando a pessoa em causa desempenha um papel na vida pública. No entanto, essa relação inverte-se quando pelo menos uma parte das informações mencionadas no pedido de supressão de referências, que não apresentam um caráter menor relativamente à totalidade do conteúdo, se revele inexata. Nessa hipótese, o direito de informar e o direito de ser informado não podem ser tidos em conta, uma vez que não podem incluir o direito de difundir e de aceder a tais informações.

Em seguida, no que respeita, por um lado, às obrigações relativas à demonstração do caráter exato ou não das informações que figuram no conteúdo apresentado, o Tribunal de Justiça especifica que cabe à pessoa que pede a supressão de referências devido à inexatidão de tais informações provar a inexatidão manifesta dessas informações ou, pelo menos, de parte dessas informações que não apresente um caráter menor relativamente à totalidade desse conteúdo. Todavia, para evitar impor a essa pessoa um ónus excessivo suscetível de prejudicar o efeito útil do direito à supressão de referências, cabe-lhe unicamente fornecer os elementos de prova que, tendo em conta as circunstâncias do caso concreto, lhe possa razoavelmente ser exigido que procure. Em princípio, esta pessoa não pode ser obrigada a apresentar, desde a fase pré-contenciosa, em apoio do seu pedido de supressão de referências, uma decisão judicial obtida contra o editor do sítio Internet, mesmo sob a forma de uma decisão proferida num processo de medidas provisórias.

Por outro lado, no que respeita às obrigações e responsabilidades impostas ao operador do motor de busca, o Tribunal de Justiça sublinha que este último, para verificar se um conteúdo pode continuar a ser incluído na lista de resultados das pesquisas efetuadas por intermédio do seu motor de busca na sequência de um pedido de supressão de referências, deve basear-se em todos os direitos e interesses envolvidos, bem como em todas as circunstâncias do caso concreto. Todavia, esse operador não pode ser obrigado a investigar os factos e, para esse efeito, a organizar um debate contraditório com o fornecedor de conteúdos para obter os elementos em falta relativamente à exatidão do conteúdo apresentado. Uma obrigação de contribuir

para demonstrar o caráter exato ou não do conteúdo apresentado faz recair sobre o referido operador um ónus que ultrapassa o que razoavelmente se pode esperar à luz das suas responsabilidades, competências e possibilidades. Esta solução comporta um sério risco de conteúdos que respondem a uma necessidade de informação legítima e preponderante do público serem suprimidos e, deste modo, se tornarem difíceis de encontrar na Internet. Assim, existiria um risco real de um efeito dissuasivo no exercício da liberdade de expressão e de informação se esse operador procedesse a uma supressão de referências de modo quase sistemático, com vista a evitar ter de suportar o ónus de investigar os factos pertinentes para determinar o caráter exato ou não do conteúdo apresentado.

Por conseguinte, quando o requerente da supressão de referências apresenta elementos de prova que demonstrem o caráter manifestamente inexato das informações que figuram no conteúdo apresentado ou, pelo menos, de uma parte dessas informações que não apresente um caráter menor relativamente à totalidade do mesmo, o operador do motor de busca está obrigado a deferir esse pedido. O mesmo acontece quando esse requerente apresenta uma decisão judicial proferida contra o editor do sítio Internet que assenta na constatação de que as informações que figuram no conteúdo apresentado, as quais não têm um caráter menor relativamente à totalidade deste conteúdo, são, pelo menos à primeira vista, inexatas. Em contrapartida, se o caráter inexato de tais informações não se revelar de modo manifesto à luz dos elementos de prova fornecidos pelo requerente, o operador do motor de busca não está obrigado, na falta de tal decisão judicial, a deferir o pedido de supressão de referências. Quando as informações em causa são suscetíveis de contribuir para um debate de interesse geral, à luz de todas as outras circunstâncias do caso em apreço, há que atribuir uma importância particular ao direito à liberdade de expressão e de informação.

Por último, o Tribunal de Justiça acrescenta que, quando o operador de um motor de busca não dá seguimento ao pedido de supressão de referências, a pessoa em causa deve poder submeter o assunto à autoridade de controlo ou à autoridade judicial, para que estes efetuem as verificações necessárias e ordenem a esse responsável a tomada de medidas em conformidade. A este respeito, é designadamente às autoridades judiciais que compete assegurar a ponderação dos interesses concorrentes, sendo estas que estão mais bem colocadas para efetuar uma ponderação complexa e aprofundada, que tenha em conta todos os critérios e todos os elementos estabelecidos pela jurisprudência pertinente.

Em segundo lugar, o Tribunal de Justiça declara que, no âmbito da ponderação dos direitos fundamentais supramencionados, para efeitos da apreciação de um pedido de supressão de referências destinado a suprimir dos resultados de uma pesquisa de imagens, efetuada a partir do nome de uma pessoa singular, as fotografias, exibidas sob a forma de imagens de pré-visualização, que representam essa pessoa, deve ter-se em conta o valor informativo dessas fotografias independentemente do contexto inicial da

sua publicação na página Internet da qual foram retiradas. No entanto, há que ter em consideração todos os elementos textuais que acompanhem diretamente a exibição dessas fotografias nos resultados de pesquisa e que sejam suscetíveis de clarificar o valor informativo das mesmas.

Para chegar a esta conclusão, o Tribunal de Justiça sublinha que as pesquisas de imagens efetuadas por intermédio de um motor de busca na Internet a partir do nome de uma pessoa estão sujeitas aos mesmos princípios que se aplicam às pesquisas de páginas Internet e das informações aí contidas. Indica que a exibição, na sequência de uma pesquisa por nome, sob a forma de imagens de pré-visualização, de fotografias da pessoa em causa, é suscetível de constituir uma ingerência particularmente importante nos direitos à proteção da vida privada e dos dados pessoais dessa pessoa.

Por conseguinte, quando é apresentado ao operador de um motor de busca um pedido de supressão de referências destinado a suprimir dos resultados de uma pesquisa de imagens, efetuada a partir do nome de uma pessoa, fotografias exibidas sob a forma de imagens de pré-visualização que representam essa pessoa, este deve verificar se a exibição das fotografias em causa é necessária ao exercício do direito à liberdade de informação dos internautas potencialmente interessados em aceder a essas fotografias através da referida pesquisa.

Ora, na medida em que o motor de busca exibe fotografias da pessoa em causa fora do contexto em que são publicadas na página Internet apresentada, na maioria das vezes para ilustrar os elementos textuais contidos nessa página, há que determinar se este contexto deve, contudo, ser tido em consideração na ponderação dos direitos e dos interesses concorrentes a realizar. Neste âmbito, a questão de saber se a referida apreciação deve igualmente incluir o conteúdo da página Internet na qual figura a fotografia relativamente à qual é pedida a remoção da exibição sob a forma de imagens de pré-visualização depende do objeto e da natureza do tratamento em causa.

No que respeita, em primeiro lugar, ao objeto do tratamento em causa, o Tribunal de Justiça observa que a publicação de fotografias como meio de comunicação não verbal é suscetível de ter um impacto maior nos internautas do que as publicações textuais. Com efeito, as fotografias são, enquanto tais, um meio importante de chamar a atenção dos internautas e podem suscitar o interesse em aceder aos artigos que ilustram. Ora, devido, nomeadamente, à circunstância de estas se prestarem frequentemente a várias interpretações, a sua exibição na lista dos resultados da pesquisa sob a forma de imagens de pré-visualização pode implicar uma ingerência particularmente grave no direito da pessoa em causa à proteção da sua imagem, o que deve ser tido em conta no âmbito da ponderação entre os direitos e os interesses concorrentes. Impõe-se uma ponderação distinta consoante estejam em causa, por um lado, artigos com fotografias publicadas pelo editor da página Internet e que, inseridos no seu contexto original, ilustram as informações fornecidas nesses artigos e as opiniões aí expressas, e, por outro, fotografias exibidas sob a forma de imagens de pré-visualização na lista de

resultados pelo operador de um motor de busca fora do contexto em que foram publicadas na página Internet de origem.

A este respeito, o Tribunal de Justiça recorda que o motivo que justifica a publicação de um dado pessoal num sítio Internet não só não coincide forçosamente com o que se aplica à atividade dos motores de busca, mas, mesmo quando isso acontece, o resultado da ponderação dos direitos e dos interesses em causa a realizar pode divergir consoante esteja em causa o tratamento efetuado pelo operador de um motor de busca ou o efetuado pelo editor dessa página Internet. Por um lado, os interesses legítimos que justificam esses tratamentos podem ser diferentes e, por outro, as consequências dos referidos tratamentos para a pessoa em causa, e designadamente para a sua vida privada, não são necessariamente os mesmos

No que respeita, em segundo lugar, à natureza do tratamento efetuado pelo operador do motor de busca, o Tribunal de Justiça constata que, ao encontrar as fotografias de pessoas singulares publicadas na Internet e ao exibi-las separadamente, nos resultados de uma pesquisa por imagens, sob a forma de imagens de pré-visualização, o operador de um motor de busca oferece um serviço no qual efetua um tratamento de dados pessoais autónomo e distinto tanto do tratamento do editor da página Internet da qual são retiradas as fotografias como do tratamento relativo à supressão de referências dessa página, pelo qual esse operador é igualmente responsável.

Por conseguinte, impõe-se uma apreciação autónoma da atividade do operador do motor de busca, que consiste em exibir resultados de uma pesquisa de imagens, sob a forma de imagens de pré-visualização, uma vez que a violação adicional dos direitos fundamentais resultante dessa atividade pode ser particularmente intensa devido à agregação, numa pesquisa por nome, de todas as informações relativas à pessoa em causa que se encontram na Internet. No âmbito dessa apreciação autónoma, há que ter em conta que a exibição na Internet de fotografias sob a forma de imagens de pré-visualização constitui, por si só, o resultado pretendido pelo internauta, independentemente da sua decisão posterior de aceder ou não à página Internet de origem.

O Tribunal de Justiça observa, todavia, que tal ponderação específica, que tem em conta a natureza autónoma do tratamento a que procede o operador do motor de busca, não prejudica a eventual pertinência de elementos textuais que podem acompanhar diretamente a exibição de uma fotografia na lista dos resultados de uma pesquisa, dado que esses elementos são suscetíveis de clarificar o valor informativo dessa fotografia para o público e, consequentemente, influenciar a ponderação dos direitos e dos interesses envolvidos.

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)

Com este acórdão, o Tribunal de Justiça 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 de Justiça 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 sobre o 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» previsto na Diretiva 2002/58 [94], em conjugação com a Diretiva 95/46 [95] e com o RGPD [96].

Em primeiro lugar, o Tribunal de Justiça observou que o artigo 2.°, alínea h), da Diretiva 95/46, 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

[94] 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).

[95] Artigo 2.°, alínea h), da Diretiva 95/46.

[96] Artigo 6.°, n.° 1, alínea a), do Regulamento 2016/679.

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 [97], cujo artigo 4.°, n.° 11, exige uma manifestação de vontade que assuma 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».

O Tribunal de Justiça 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 de Justiça acrescentou que o facto de esse utilizador ativar o botão de participação no jogo promocional em causa não pode ser suficiente para considerar que deu validamente o seu consentimento à colocação de cookies.

Em segundo lugar, o Tribunal de Justiça constatou que o artigo 5.°, n.° 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. Daqui 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.

Em terceiro lugar, o Tribunal de Justiça salientou que o artigo 5.°, n.° 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 de Justiça 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.

97 *IDEM.*

5. Tratamento de dados pessoais nas redes sociais em linha

Acórdão de 4 de julho de 2023 (Grande Secção), Meta Platforms e o. (Condições gerais de utilização de uma rede social) (C-252/21, EU:C:2023:537)

A sociedade Meta Platforms é proprietária da rede social em linha «Facebook», que é gratuita para os utilizadores privados. O modelo económico desta rede social baseia-se no financiamento através da publicidade em linha, feita por medida para os seus utilizadores individuais. Esta publicidade é tecnicamente possível através da criação automatizada de perfis pormenorizados dos utilizadores da rede e dos serviços em linha propostos ao nível do grupo Meta. Assim, para poder utilizar a referida rede social, os utilizadores devem, no momento do seu registo, aceitar as condições gerais estabelecidas pela Meta Platforms, que remetem para as políticas de utilização dos dados e dos testemunhos de conexão (*cookies*) fixados pela referida sociedade. Ao abrigo destas últimas, além dos dados que esses utilizadores fornecem diretamente ao registarem-se, a Meta Platforms recolhe também dados relativos às atividades desses utilizadores dentro e fora da rede social e cruza esses dados com as contas Facebook dos utilizadores em causa. Quanto a estes últimos dados, também designados «dados *off*-Facebook», trata-se, por um lado, dos dados relativos à consulta de páginas Internet e de aplicações de terceiros, e, por outro, dos dados relativos à utilização dos outros serviços em linha pertencentes ao grupo Meta (entre os quais o Instagram e o WhatsApp). A síntese global destes dados permite tirar conclusões detalhadas sobre as preferências e os interesses desses mesmos utilizadores.

Por Decisão de 6 de fevereiro de 2019, a Bundeskartellamt (Autoridade Federal da Concorrência, Alemanha) proibiu a Meta Platforms, por um lado, de sujeitar, nas condições gerais em vigor, a utilização da rede social Facebook por utilizadores privados residentes na Alemanha ao tratamento dos seus dados *off*-Facebook e de proceder, sem o seu consentimento, ao tratamento desses dados Além disso, a Autoridade Federal da Concorrência impôs-lhes que adaptassem essas condições gerais de modo a delas resultar claramente que os referidos dados não serão recolhidos, cruzados com as contas de utilizadores Facebook nem utilizados sem o consentimento do utilizador em causa. Por último, essa autoridade sublinhou que esse consentimento não era válido quando constituía uma condição para a utilização da rede social. Fundamentou a sua decisão no facto de o tratamento dos dados dos utilizadores em causa, que não está em conformidade com o RGPD, constituir uma exploração abusiva da posição dominante da Meta Platforms no mercado das redes sociais em linha.

A Meta Platforms interpôs recurso dessa decisão no Oberlandesgericht Düsseldorf (Tribunal Regional Superior de Düsseldorf, Alemanha). Tendo dúvidas, designadamente, quanto à interpretação e aplicação de algumas disposições deste regulamento, o Tribunal Regional Superior de Düsseldorf apresentou um pedido de decisão prejudicial ao Tribunal de Justiça.

Com o seu acórdão, o Tribunal de Justiça, reunido em Grande Secção, presta esclarecimentos sobre a possibilidade de tratamento, por um operador de uma rede social, de dados pessoais «sensíveis» dos seus utilizadores, sobre as condições de licitude do tratamento de dados efetuado por esse operador, bem como sobre a validade do consentimento, dado para efeitos desse tratamento por esses utilizadores, a uma empresa em posição dominante no mercado nacional das redes sociais em linha.

Quanto ao tratamento de categorias especiais de dados pessoais [98], o Tribunal de Justiça considera que, no caso de um utilizador de uma rede social em linha consultar sítios Internet ou aplicações relacionadas com uma ou várias dessas categorias e, se for caso disso, aí inserir dados, registando-se ou efetuando encomendas em linha, o tratamento de dados pessoais pelo operador dessa rede social em linha [99] deve ser considerado um «tratamento de categorias especiais de dados pessoais», na aceção do artigo 9.°, n.° 1, do RGPD, quando permita revelar informações abrangidas por uma dessas categorias específicas, independentemente de essas informações dizerem respeito a um utilizador dessa rede ou a qualquer outra pessoa singular. Esse tratamento de dados é, em princípio, proibido, sob reserva de certas derrogações [100].

A este último respeito, o Tribunal de Justiça especifica que, quando o utilizador de uma rede social consulte sítios Internet ou aplicações relativamente a uma ou várias das categorias especiais de dados, não torna manifestamente públicos [101] os dados relativos a essa consulta, recolhidos pelo operador dessa rede social em linha através de *cookies* ou de tecnologias de registo semelhantes. Por outro lado, quando insere dados em tais sítios Internet ou em tais aplicações ou quando ativa botões de seleção integrados nesses sítios ou nessas aplicações, como os botões «gosto» ou «partilhar» ou os botões que permitem ao utilizador identificar-se nesses sítios ou nessas aplicações utilizando as credenciais de conexão associadas à sua conta de utilizador da rede social, o seu número de telefone ou o seu endereço de correio eletrónico, esse utilizador só torna manifestamente públicos os dados assim inseridos ou resultantes da ativação desses botões no caso de ter manifestado expressamente a sua escolha prévia, eventualmente com base numa parametrização individual efetuada com pleno conhecimento de causa,

---

98 Referidas no artigo 9.°, n.° 1, do RGPD. Esta disposição prevê que «[é] proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa».

99 Esse tratamento consiste na recolha, através de interfaces integradas, de *cookies* ou de tecnologias de registo semelhantes, dos dados provenientes da consulta desses sítios e dessas aplicações bem como dos dados inseridos pelo utilizador, no cruzamento do conjunto desses dados com a conta da rede social desse utilizador e na utilização dos referidos dados por esse operador.

100 Previstas no artigo 9.°, n.° 2, do RGPD. Esta disposição prevê: «O disposto no n.° 1 não se aplica se se verificar um dos seguintes casos:
a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.° 1 não pode ser anulada pelo titular dos dados;
e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da suas função jurisdicional;
[...]».

101 Na aceção do artigo 9.°, n.° 2, alínea e), do RGPD.

de tornar os dados que lhe dizem respeito publicamente acessíveis a um número ilimitado de pessoas.

No que diz mais genericamente respeito às condições de licitude do tratamento de dados pessoais, o Tribunal de Justiça recorda que, nos termos do RGPD, o tratamento de dados pessoais é lícito se e na medida em que o titular dos dados tiver dado o seu consentimento para uma ou mais finalidades específicas [102]. Não tendo esse consentimento sido prestado, ou quando esse consentimento não tenha sido dado de forma livre, específica, informada e inequívoca, esse tratamento é, não obstante, justificado quando cumpre um dos requisitos de necessidade [103], que devem ser interpretados de forma estrita. Ora, o tratamento de dados pessoais dos seus utilizadores efetuado pelo operador de uma rede social em linha só pode ser considerado necessário para a execução de um contrato do qual os titulares de dados são partes se esse tratamento for objetivamente indispensável para realizar uma finalidade que faça parte integrante da prestação contratual destinada a esses mesmos utilizadores, de modo que o objeto principal do contrato não poderia ser alcançado sem esse tratamento.

Além disso, segundo o Tribunal de Justiça, o tratamento de dados em causa só pode ser considerado necessário para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por um terceiro, na aceção desta disposição, desde que o referido operador tenha indicado aos utilizadores cujos dados foram recolhidos um interesse legítimo prosseguido pelo seu tratamento, esse tratamento seja efetuado na estrita medida do necessário para a realização desse interesse legítimo e resulte de uma ponderação dos interesses opostos, à luz de todas as circunstâncias pertinentes, que os interesses ou os direitos ou as liberdades fundamentais desses utilizadores não prevalecem sobre o referido interesse legítimo do responsável pelo tratamento ou de um terceiro. Ora, o Tribunal de Justiça considera nomeadamente que, na falta de consentimento dos referidos utilizadores, os seus interesses e direitos fundamentais prevalecem sobre o interesse do operador de uma rede social em linha na personalização da publicidade através da qual financia a sua atividade.

Por último, o Tribunal de Justiça especifica que o tratamento de dados em causa é justificado quando for efetivamente necessário para o cumprimento de uma obrigação jurídica à qual o responsável pelo tratamento está sujeito, por força de uma disposição do direito da União ou do direito do Estado-Membro em causa, quando esse fundamento jurídico responda a um objetivo de interesse público e seja proporcionado

[102] Nos termos do artigo 6.°, n.° 1, primeiro parágrafo, alínea a), do RGPD.

[103] Mencionados no artigo 6.°, n.° 1, primeiro parágrafo, alíneas b) a f), do RGPD. Ao abrigo destas disposições, o tratamento só é lícito se e na medida em que seja, nomeadamente, necessário para a execução de um contrato do qual os titulares de dados são partes [artigo 6.°, n.° 1, primeiro parágrafo, alínea b), do RGPD], para o cumprimento de uma obrigação jurídica à qual o responsável pelo tratamento está sujeito [artigo 6.°, n.° 1, primeiro parágrafo, alínea c), do RGPD] ou para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por um terceiro [artigo 6.°, n.° 1, primeiro parágrafo, alínea f), do RGPD].

ao objetivo legítimo prosseguido e quando esse tratamento seja efetuado na estrita medida do necessário.

Enfin, la Cour précise que le traitement de données en cause est justifié lorsqu'il est effectivement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, en vertu d'une disposition du droit de l'Union ou du droit de l'État membre concerné, que cette base juridique répond à un objectif d'intérêt public et est proportionnée à l'objectif légitime poursuivi et que ce traitement est opéré dans les limites du strict nécessaire.

No que se refere à validade do consentimento dos utilizadores em causa no tratamento dos seus dados ao abrigo do RGPD, o Tribunal de Justiça considera que a circunstância de o operador de uma rede social em linha ocupar uma posição dominante no mercado das redes sociais em linha não obsta, enquanto tal, a que os utilizadores dessa rede possam validamente consentir no tratamento dos seus dados pessoais, efetuado por esse operador. Não obstante, uma vez que é suscetível de afetar a liberdade de escolha desses utilizadores e criar um desequilíbrio manifesto entre os mesmos e o referido operador, esta circunstância constitui um elemento importante para determinar se o consentimento foi efetivamente dado de forma válida e, nomeadamente, livre, o que incumbe ao referido operador provar [104].

Em especial, os utilizadores da rede social em questão devem dispor da liberdade de recusar individualmente, no âmbito do processo contratual, dar o seu consentimento a operações específicas de tratamento de dados não necessárias à execução do contrato, sem que, no entanto, sejam obrigados a renunciar integralmente à utilização dessa rede social em linha, o que implica que seja proposta aos referidos utilizadores, sendo caso disso mediante uma remuneração adequada, uma alternativa equivalente não acompanhada de tais operações de tratamento de dados. Além disso, deve poder ser dado um consentimento distinto para o tratamento dos dados *off*-Facebook.

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)

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

[104] Por força do artigo 7.°, n.° 1, do RGPD.

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.°, n.° 1, segundo parágrafo, da Diretiva 95/46.

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 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 de Justiça 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.

O Tribunal de Justiça 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 de Justiça, a tutela do Estado exercida sobre as autoridades nacionais de controlo não é, por conseguinte, compatível com a exigência de independência.

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 de Justiça declarou 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.

O Tribunal de Justiça recordou, antes de mais, que a expressão «com total independência» constante do artigo 28.°, n.° 1, segundo parágrafo, da Diretiva 95/46, implica que as autoridades de controlo devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. A este respeito, 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.

O Tribunal de Justiça precisou que, para poder cumprir o critério de independência enunciado na referida disposição da Diretiva 95/46, uma autoridade nacional de controlo não tem de 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.

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

Neste processo, a Comissão pedia ao Tribunal de Justiça 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 de Justiça 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.

Com efeito, segundo o Tribunal de Justiça, 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.

Além disso, o Tribunal de Justiça 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, atuar acima de qualquer suspeita de parcialidade.

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)

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 ter comunicado esses dados a agências de recuperação de crédito com vista a obter a regularização 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 de cassação, 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 28.° da Diretiva 95/46. Consequentemente, submeteu várias questões prejudiciais ao Tribunal de Justiça.

No que respeita ao direito nacional aplicável, o Tribunal de Justiça 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 o facto, por um lado, de 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 causa. Em contrapartida, o Tribunal de Justiça considerou que a questão da nacionalidade das pessoas afetadas por esse tratamento de dados é desprovida de pertinência.

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 de Justiça 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. 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.

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 (v. igualmente a rubrica IV, intitulada «Transferência de dados pessoais para países terceiros»), o Tribunal de Justiça 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 de Justiça começou por declarar 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.

No que diz respeito ao poder de controlar as transferências de dados pessoais para os países terceiros, o Tribunal de Justiça 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.

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.

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 de Justiça 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 de Justiça 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).

Além disso, o Tribunal de Justiça 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.

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 [105] 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

[105] Por exemplo, os botões «gosto» ou «partilhar».

informado os 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 dessa decisão para o hof van beroep te Brussel (Tribunal de Recurso de Bruxelas, Bélgica), órgão jurisdicional de reenvio no presente processo. Nesse órgão jurisdicional, a Autoridade de Proteção de Dados belga (a seguir «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 [106] 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.

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 [107], embora não seja a autoridade de controlo principal responsável por esse tratamento.

Em primeiro lugar, o Tribunal de Justiça 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,

106 Nos termos do artigo 56.°, n.° 1, do RGPD: «Sem prejuízo do disposto no artigo 55.°, 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.»

107 Na aceção do artigo 4.°, ponto 23, do RGPD.

por outro, este poder deve ser exercido respeitando os procedimentos de cooperação e de controlo da coerência previstos neste regulamento [108].

Com efeito, no que respeita aos tratamentos transfronteiriços, o RGPD prevê o mecanismo do «balcão único» [109], que se baseia numa repartição das competências entre uma «autoridade de 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 de 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 [110], ao passo que a competência das outras autoridades nacionais de controlo para adotarem tal decisão, ainda que a título provisório, constitui a exceção [111]. 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.

O Tribunal de Justiça 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 ao RGPD às autoridades jurisdicionais deste Estado e 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 [112] é conforme com os artigos 7.°, 8.° e 47.° da Carta, 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.

Em segundo lugar, o Tribunal de Justiça declara que, no 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 [113] 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

[108] Previstos nos artigos 56.° e 60.° do RGPD.
[109] Artigo 56.°, n.° 1, do RGPD.
[110] Artigo 60.°, n.° 7, do RGPD.
[111] O artigo 56.°, n.° 2, e o artigo 66.° do RGPD consagram as exceções ao princípio da competência decisória da autoridade de controlo principal.
[112] Previstas nos artigos 55.° e 56.°, lidos em conjunto com o artigo 60.° do RGPD.
[113] Nos termos do artigo 58.°, n.° 5, do RGPD.

desse Estado-Membro. No entanto, o exercício deste poder deve ser abrangido pelo âmbito de aplicação territorial do RGPD [114], o que pressupõe que o responsável pelo tratamento ou o subcontratante para o tratamento transfronteiriço disponha de um estabelecimento no território da União.

Em terceiro lugar, o Tribunal de Justiça declara que, no 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 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 a referida autoridade seja competente para exercer esse poder.

No entanto, o Tribunal de Justiça precisa que o exercício deste poder pressupõe que o RGPD seja aplicável. No caso em apreço, 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, abrangido pelo âmbito de aplicação do RGPD.

Em quarto lugar, o Tribunal de Justiça 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, esta 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 por 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.

Em quinto lugar e último lugar, o Tribunal de Justiça 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

[114] 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».

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.

Acórdão de 16 de janeiro de 2024 (Grande Secção), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Neste processo (v. igualmente rubrica II.1, intitulada «Âmbito de aplicação da regulamentação geral»), o Tribunal de Justiça salienta que as disposições do RGPD relativas à competência das autoridades de controlo nacionais e ao direito de reclamação [115] não necessitam da adoção de medidas nacionais de aplicação e são suficientemente claras, precisas e incondicionais para produzirem efeito direto. Daqui se conclui que, embora o RGPD reconheça uma margem de apreciação aos Estados-Membros quanto ao número de autoridades de controlo a instituir [116], fixa, em contrapartida, o alcance das suas competências para fiscalizar a aplicação do RGPD. Assim, no caso de um Estado-Membro decidir instituir uma única autoridade nacional de controlo, esta dispõe necessariamente da totalidade das competências previstas neste regulamento. Qualquer outra interpretação poria em causa o efeito útil destas disposições e poderia enfraquecer o efeito útil de todas as outras disposições do RGPD suscetíveis de ser afetadas por uma reclamação.

No que respeita à circunstância de as disposições nacionais de ordem constitucional excluírem a possibilidade de uma autoridade de controlo que depende do poder executivo fiscalizar a aplicação do RGPD por um organismo do poder legislativo, o Tribunal de Justiça sublinha que é precisamente no respeito da estrutura constitucional dos Estados-Membros que o RGPD se limita a exigir destes últimos que instituam pelo menos uma autoridade de controlo, dando-lhes a possibilidade de instituírem várias. Este regulamento reconhece assim aos Estados-Membros uma margem de apreciação que lhes permite criar tantas autoridades de controlo quantas sejam requeridas, nomeadamente, pelas exigências relativas à sua estrutura constitucional.

Além disso, a invocação de disposições de direito nacional por um Estado-Membro não pode afetar a unidade e a eficácia do direito da União. Efetivamente, os efeitos associados ao princípio do primado do direito da União impõem-se a todos os órgãos de um Estado-Membro, sem que, nomeadamente, as disposições internas, incluindo de ordem constitucional, o possam impedir.

[115] Respetivamente, artigo 55.°, n.° 1, e artigo 77.°, n.° 1, do RGPD.
[116] Em conformidade com o artigo 51,°, n.° 1, do RGPD.

Assim, quando um Estado-Membro tenha optado por instituir uma única autoridade de controlo, não pode invocar disposições de direito nacional, ainda que sejam de ordem constitucional, para excluir do controlo dessa autoridade tratamentos de dados pessoais abrangidos pelo âmbito de aplicação do RGPD.

4. Condições de aplicação de coimas

Acórdão de 5 de dezembro de 2023 (Grande Secção), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Neste processo (v. igualmente rubricas II.3, II.5 e II.6., intituladas «Conceito de "tratamento de danos pessoais"», «Conceito de "responsável pelo tratamento de dados pessoais" e «Conceito de "responsável conjunto pelo tratamento de dados pessoais"»), o Tribunal de Justiça declara que, nos termos do artigo 83.° do RGPD, só pode ser aplicada uma coima a um responsável pelo tratamento se se demonstrar que cometeu, intencionalmente ou por negligência, uma violação das regras contidas neste regulamento [117].

A este respeito, o Tribunal de Justiça especifica que o legislador da União não deixou aos Estados-Membros uma margem de apreciação no que respeita às condições substantivas que devem ser respeitadas por uma autoridade de controlo quando decide aplicar uma coima a um responsável pelo tratamento ao abrigo desta disposição. O facto de o RGPD dar aos Estados-Membros a possibilidade de preverem exceções em relação às autoridades e organismos públicos estabelecidos no seu território [118], e exigências relativas ao procedimento a seguir pelas autoridades de controlo para aplicar uma coima [119] não significa de modo nenhum que esses Estados estão também habilitados para prever tais condições substantivas.

No que respeita a estas condições, o Tribunal de Justiça observa que entre os elementos enumerados no RGPD à luz dos quais a autoridade de controlo aplica uma coima ao responsável pelo tratamento figura «[o] caráter intencional ou negligente da infração» [120]. Em contrapartida, nenhum destes elementos prevê qualquer possibilidade de responsabilizar o responsável pelo tratamento na ausência de um comportamento culposo da sua parte. Assim, só as violações das disposições do RGPD cometidas pelo responsável pelo tratamento intencionalmente ou por negligência podem conduzir a que lhe seja aplicada uma coima nos termos do artigo 83.° deste regulamento.

---

117 Violação referida no artigo 83.°, n.os 4 a 6.

118 Nos termos do artigo 83.°, n.° 7, do RGPD que dispõe que «[...] os Estados-Membros podem prever normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos estabelecidos no seu território».

119 Nos termos do artigo 83.°, n.° 8, do RGPD, lido à luz do seu considerando 129.

120 Artigo 83.°, n.° 2, alínea b), do RGPD.

O Tribunal de Justiça acrescenta que esta interpretação é corroborada pela sistemática geral e pela finalidade do RGPD. Neste contexto, especifica que a existência de um sistema de sanções ao abrigo do RGPD que permite aplicar, quando as circunstâncias específicas de cada caso em apreço o justifiquem, uma coima gera, para os responsáveis pelo tratamento e os subcontratantes, um incentivo ao cumprimento deste regulamento e que, através do seu efeito dissuasivo, as coimas contribuem para o reforço da proteção das pessoas em causa. No entanto, o legislador da União não considerou necessário prever a aplicação de coimas na ausência de culpa. Atendendo ao facto de o RGPD visar um nível de proteção simultaneamente equivalente e homogéneo e que deve, para esse fim, ser aplicado de forma coerente em toda a União, seria contrário a esta finalidade permitir aos Estados-Membros preverem tal regime de aplicação de uma coima.

Além disso, o Tribunal de Justiça conclui que uma coima pode ser aplicada a um responsável pelo tratamento relativamente a operações de tratamento de dados pessoais realizadas por um subcontratante por sua conta, salvo se, no âmbito dessas operações este subcontratante tiver realizado tratamentos para finalidades que lhe são próprias ou tiver tratado esses dados de maneira incompatível com o quadro ou com as modalidades de tratamento conforme tinham sido determinadas pelo responsável pelo tratamento, ou de tal forma que não se possa razoavelmente considerar que a pessoa responsável teria dado o seu consentimento. Nesta hipótese, o subcontratante deve ser considerado responsável pelo tratamento.

Acórdão de 5 de dezembro de 2023 (Grande Secção), Deutsche Wohnen (C-807/21, EU:C:2023:950)

A Deutsche Wohnen SE (a seguir «DW») é uma sociedade imobiliária que detém indiretamente, através de participações em diferentes sociedades, numerosas unidades comerciais e habitacionais. No âmbito das suas atividades comerciais, trata dados pessoais dos arrendatários das referidas unidades.

Na sequência de dois controlos efetuados em 2017 e em 2019, a Berliner Beauftragte für den Datenschutz (Autoridade de Controlo em Matéria de Proteção de Dados de Berlim, Alemanha) constatou que a DW tinha cometido uma série de infrações ao RGPD. Por Decisão de 30 de outubro de 2019, a referida autoridade de controlo aplicou-lhe, a esse título, coimas.

A DW interpôs recurso dessa decisão no Landgericht Berlin (Tribunal Regional de Berlim, Alemanha), que arquivou o processo. Este órgão jurisdicional salientou que, por força da lei alemã [121], uma infração administrativa só pode ser declarada contra uma pessoa

[121] Gesetz über Ordnungswidrigkeiten (Lei relativa às Infrações Administrativas), de 24 de maio de 1968 (BGBl. 1968 I, p. 481), na versão da comunicação de 19 de fevereiro de 1987 (BGBl. 1987 I, p. 602), conforme alterada pela Lei de 19 de junho de 2020 (BGBl. 2020 I, p. 1350).

singular e não contra uma pessoa coletiva. Além disso, em caso de responsabilização de uma pessoa coletiva, apenas os atos dos órgãos ou dos representantes da mesma lhe podem ser imputados. O Staatsanwaltschaft Berlin (Ministério Público de Berlim) interpôs recurso desta decisão para o Kammergericht Berlin (Tribunal Regional Superior de Berlim, Alemanha). Nestas circunstâncias, o referido órgão jurisdicional submeteu ao Tribunal de Justiça um pedido de decisão prejudicial relativo à interpretação do RGPD.

No seu acórdão, o Tribunal de Justiça, reunido em Grande Secção, pronuncia-se sobre as condições de aplicação de coimas a título do RGPD. Em primeiro lugar, analisa a questão de saber se os Estados-Membros podem subordinar a aplicação de uma coima a uma pessoa coletiva à condição de a infração ao referido regulamento ser previamente imputada a uma pessoa singular identificada. Em segundo lugar, debruça-se também, à à semelhança do Acórdão Nacionalinis visuomenės sveikatos centras (v. *supra*) sobre a questão de saber se a infração às disposições do RGPD que é objeto de sanção tem de ter sido cometida intencionalmente ou por negligência

No que respeita à aplicação de uma coima por força do RGPD a uma pessoa coletiva, o Tribunal de Justiça salienta, antes de mais, que os princípios, proibições e obrigações previstos no RGPD têm por destinatários, em especial, os «responsáveis pelo tratamento» cuja responsabilidade se estende a qualquer tratamento de dados pessoais realizado por estes ou por sua conta. É esta responsabilidade que constitui, em caso de violação das disposições do RGPD, o fundamento para a aplicação de uma coima ao responsável pelo tratamento em aplicação do artigo 83.° do referido regulamento. No entanto, o legislador da União, para efeitos da determinação de tal responsabilidade, não efetuou uma distinção entre as pessoas singulares e as pessoas coletivas, dado que a referida responsabilidade está sujeita unicamente à condição de estas, individualmente ou em conjunto com outras, determinarem as finalidades e os meios do tratamento de dados pessoais [122]. Por conseguinte, em princípio, qualquer pessoa que preencha esta condição é nomeadamente responsável por qualquer infração ao RGPD, realizada por si mesma ou por sua conta. Isso implica, por um lado, que as pessoas coletivas são responsáveis não só pelas infrações cometidas pelos seus representantes, diretores ou gestores, mas também por qualquer outra pessoa que atue no âmbito da atividade comercial dessas pessoas coletivas e por sua conta. Por outro lado, as coimas previstas pelo RGPD em caso de tais infrações devem poder ser aplicadas diretamente a pessoas coletivas quando estas possam ser qualificadas de responsáveis pelo tratamento.

Em seguida, o Tribunal de Justiça observa que nenhuma disposição do RGPD permite considerar que a aplicação de uma coima a uma pessoa coletiva enquanto responsável pelo tratamento esteja sujeita à constatação prévia de que essa infração foi cometida por uma pessoa singular identificada. Além disso, o legislador da União não deixou aos

[122] Nos termos do artigo 4.°, ponto 7, do RGPD.

Estados-Membros margem de apreciação a este respeito. O facto de o RGPD dar aos Estados-Membros a possibilidade de estabelecerem exigências no que respeita ao procedimento a seguir pelas autoridades de controlo para aplicar uma coima [123] não significa, de modo nenhum, que estes estão igualmente habilitados a prever condições materiais adicionais às fixadas pelo RGPD.

Neste contexto, o Tribunal de Justiça especifica que permitir aos Estados-Membros que exijam, unilateralmente e como condição necessária à aplicação de uma coima nos termos do artigo 83.° do RGPD a um responsável pelo tratamento que é uma pessoa coletiva, que a violação em causa seja imputada ou imputável, previamente, a uma pessoa singular identificada seria contrário à finalidade do RGPD. Além disso, tal exigência adicional poderia, em última análise, enfraquecer a eficácia e o efeito dissuasivo das coimas aplicadas a pessoas coletivas enquanto responsáveis pelo tratamento.

Por último, o Tribunal de Justiça salienta que o conceito de «empresa», na aceção dos artigos 101.° e 102.° TFUE [124], não tem incidência na questão de saber se e em que condições pode ser aplicada uma coima nos termos do RGPD a um responsável pelo tratamento que seja uma pessoa coletiva e só é pertinente para determinar o montante da referida coima.

Assim, o Tribunal de Justiça concluiu que o RGPD [125] se opõe a uma regulamentação nacional por força da qual só pode ser aplicada uma coima a uma pessoa coletiva na sua qualidade de responsável pelo tratamento por uma infração prevista neste regulamento [126] quando essa infração tenha sido previamente imputada a uma pessoa singular identificada.

No que respeita à questão de saber se os Estados-Membros podem prever a aplicação de uma coima mesmo quando a infração objeto de sanção não foi cometida intencionalmente ou por negligência, o Tribunal de Justiça recorda, antes de mais, que as condições materiais que devem ser respeitadas por uma autoridade de controlo quando aplica uma coima a um responsável pelo tratamento são unicamente abrangidas pelo direito da União e que os Estados-Membros não dispõem de nenhuma margem de manobra a este respeito. Seguindo um raciocínio idêntico ao adotado no Acórdão Nacionalinis visuomenės sveikatos centras acima referido, o Tribunal de Justiça declara que, por força do artigo 83.° do RGPD, só pode ser aplicada uma coima se se demonstrar que o responsável pelo tratamento, que é simultaneamente uma pessoa coletiva e uma empresa, cometeu, intencionalmente ou por negligência, uma infração às normas constantes do referido regulamento.

---

123 Como resulta do artigo 58.°, n.° 4, e do artigo 83.°, n.° 8, do RGPD, lidos à luz do considerando 129 do mesmo regulamento.
124 Para o qual remete o considerando 150 do RGPD.
125 Artigo 58.°, n.° 2, alínea i), e artigo 83.°, n.os 1 a 6, do RGPD.
126 Prevista no artigo 83.°, n.os 4 a 6, do RGPD.

5. Articulação das competências das autoridades nacionais de controlo com as competências das outras autoridades nacionais

Acórdão de 4 de julho de 2023 (Grande Secção), Meta Platforms e o. (Condições gerais de utilização de uma rede social) (C-252/21, EU:C:2023:537)

Neste processo (v. igualmente rubrica V.5., intitulada «Tratamento de dados pessoais nas redes sociais em linha»), pronunciando-se sobre a competência de uma autoridade nacional da concorrência para declarar a não conformidade de um tratamento de dados pessoais com o RGPD, o Tribunal de Justiça salienta que, sob reserva do cumprimento da sua obrigação de cooperação leal [127] com as autoridades de controlo da proteção de dados, essa autoridade pode constatar, no âmbito do exame de um abuso de posição dominante por parte de uma empresa [128], que as condições gerais de utilização dessa empresa relativas ao tratamento de dados pessoais e à sua aplicação não estão em conformidade com este regulamento, quando essa constatação seja necessária para demonstrar a existência de tal abuso. No entanto, quando uma autoridade da concorrência assinala uma violação do RGPD no âmbito da constatação de um abuso de posição dominante, não se substitui às autoridades de controlo.

Assim, tendo em conta o princípio da cooperação leal, quando as autoridades nacionais da concorrência são levadas, no exercício das suas competências, a examinar a conformidade de um comportamento de uma empresa com as disposições do RGPD, devem concertar-se e cooperar lealmente com as respetivas autoridades nacionais de controlo ou com a autoridade de controlo principal. Todas estas autoridades estão então obrigadas a respeitar os respetivos poderes e competências, de modo que as obrigações decorrentes do RGPD e os objetivos deste regulamento sejam cumpridos e o seu efeito útil seja preservado. Daqui resulta que, quando, no âmbito do exame destinado a constatar a existência de um abuso de posição dominante por parte de uma empresa, uma autoridade nacional da concorrência considere que é necessário examinar a conformidade de um comportamento dessa empresa com as disposições do RGPD, a referida autoridade deve verificar se esse comportamento ou um comportamento semelhante já foi objeto de uma decisão pela autoridade nacional de controlo competente ou pela autoridade de controlo principal ou ainda pelo Tribunal de Justiça. Se for esse o caso, a autoridade nacional da concorrência não se pode afastar dessa decisão, permanecendo livre de daí retirar as suas próprias conclusões do ponto de vista da aplicação do direito da concorrência.

---

[127] Consagrada no artigo 4.º, n.º 3, TUE.
[128] Na aceção do artigo 102.º TFUE.

Quando tenha dúvidas sobre o alcance da apreciação feita pela autoridade nacional de controlo competente ou pela autoridade de controlo principal, quando o comportamento em causa ou um comportamento semelhante seja, ao mesmo tempo, objeto de um exame por parte dessas autoridades, ou ainda quando, não tendo as referidas autoridades realizado uma investigação, considere que um comportamento de uma empresa não está em conformidade com as disposições do RGPD, a autoridade nacional da concorrência deve consultar essas autoridades e solicitar a respetiva cooperação, a fim de dissipar as suas dúvidas ou determinar se deve aguardar pela adoção de uma decisão por parte da autoridade de controlo interessada antes de iniciar a sua própria apreciação. Na falta de objeção da sua parte ou de resposta num prazo razoável, a autoridade da concorrência pode prosseguir a sua própria investigação.

TRIBUNAL DE JUSTIÇA
DA UNIÃO EUROPEIA

Direção da Investigação e Documentação

Julho 2024