



Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

6 de outubro de 2015*

«Reenvio prejudicial — Dados pessoais — Proteção das pessoas singulares no que diz respeito ao tratamento desses dados — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.º, 8.º e 47.º — Diretiva 95/46/CE — Artigos 25.º e 28.º — Transferência de dados pessoais para países terceiros — Decisão 2000/520/CE — Transferência de dados pessoais para os Estados Unidos — Nível de proteção inadequado — Validade — Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos — Poderes das autoridades nacionais de controlo»

No processo C-362/14,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pela High Court (Supremo Tribunal de Justiça, Irlanda), por decisão de 17 de julho de 2014, que deu entrada no Tribunal de Justiça em 25 de julho de 2014, no processo

Maximillian Schrems

contra

Data Protection Commissioner,

sendo interveniente:

Digital Rights Ireland Ltd,

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: V. Skouris, presidente, K. Lenaerts, vice-presidente, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (relator), S. Rodin, K. Jürimäe, presidentes de secção, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen e C. Lycourgos, juízes,

advogado-geral: M. Y. Bot,

secretária: L. Hewlett, administradora principal,

vistos os autos e após a audiência de 24 de março de 2015,

vistas as observações apresentadas:

— em representação de M. Schrems, por N. Travers, SC, P. O’Shea, BL, G. Rudden, solicitor e H. Hofmann, Rechtsanwalt,

* Língua do processo: inglês.

- em representação do Data Protection Commissioner, por P. McDermott, BL, S. More O’Ferrall e D. Young, solicitors,
- em representação da Digital Rights Ireland Ltd, por F. Crehan, BL, S. McGarr e E. McGarr, solicitors,
- em representação da Irlanda, por A. Joyce, B. Coughlan e E. Creedon, na qualidade de agentes, assistidos por D. Fennelly, BL,
- em representação do Governo belga, por J.-C. Halleux e C. Pochet, na qualidade de agentes,
- em representação do Governo checo, por M. Smolek e J. Vlácil, na qualidade de agentes,
- em representação do Governo italiano, por G. Palmieri, na qualidade de agente, assistida por P. Gentili, avvocato dello Stato,
- em representação do Governo austríaco, por G. Hesse e G. Kunnert, na qualidade de agentes,
- em representação do Governo polaco, por M. Kamejsza, M. Pawlicka e B. Majczyna, na qualidade de agentes,
- em representação do Governo esloveno, por A. Grum e V. Klemenc, na qualidade de agentes,
- em representação do Governo do Reino Unido, por L. Christie e J. Beeko, na qualidade de agentes, assistidos por J. Holmes, barrister,
- em representação do Parlamento Europeu, por D. Moore, A. Caiola e M. Pencheva, na qualidade de agentes,
- em representação da Comissão Europeia, por B. Schima, B. Martenczuk, B. Smulders e J. Vondung, na qualidade de agentes,
- em representação da Autoridade Europeia para a Proteção de Dados (AEPD), por C. Docksey, A. Buchta e V. Pérez Asinari, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 23 de setembro de 2015,

profere o presente

Acórdão

- 1 O pedido de decisão prejudicial tem por objeto a interpretação, à luz dos artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»), dos artigos 25.º, n.º 6, e 28.º da 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 L 281, p. 31), conforme alterada pelo Regulamento (CE) n.º 1882/2003 do Parlamento Europeu e do Conselho, de 29 de setembro de 2003 (JO L 284, p. 1, a seguir «Diretiva 95/46»), bem como, em substância, a validade da Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46, 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 L 215, p. 7).

- 2 Este pedido foi apresentado no âmbito de um litígio que opõe M. Schrems ao Data Protection Commissioner (comissário para a proteção de dados, a seguir «Commissioner»), a propósito da recusa deste último em investigar uma queixa apresentada por M. Schrems pelo facto de a Facebook Ireland Ltd (a seguir «Facebook Ireland») transferir para os Estados Unidos dados pessoais dos seus utilizadores e os conservar em servidores situados neste país.

Quadro jurídico

Diretiva 95/46

- 3 Os considerandos 2, 10, 56, 57, 60, 62 e 63 da diretiva 95/46 têm a seguinte redação:

«(2) [...] os sistemas de tratamento de dados estão ao serviço do Homem; [...] devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o [...] bem-estar dos indivíduos;

[...]

(10) [...] o objetivo das legislações nacionais relativas ao tratamento de dados pessoais é assegurar o respeito dos direitos e liberdades fundamentais, nomeadamente do direito à vida privada, reconhecido não só no artigo 8.º da Convenção europeia para a proteção dos direitos do Homem e das liberdades fundamentais [, assinada em Roma em 4 de novembro de 1950,] como nos princípios gerais do direito comunitário; [...] por este motivo, a aproximação das referidas legislações não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na Comunidade;

[...]

(56) [...] os fluxos transfronteiras de dados pessoais são necessários ao desenvolvimento do comércio internacional; [...] a proteção das pessoas garantida na Comunidade pela presente diretiva não obsta às transferências de dados pessoais para países terceiros que assegurem um nível de proteção adequado; [...] o caráter adequado do nível de proteção oferecido por um país terceiro deve ser apreciado em função de todas as circunstâncias associadas à transferência ou a uma categoria de transferências;

(57) [...] em contrapartida, [...] sempre que um país terceiro não ofereça um nível de proteção adequado, a transferência de dados pessoais para esse país deve ser proibida;

[...]

(60) [...] em todo o caso, as transferências para países terceiros só podem ser efetuadas no pleno respeito das disposições adotadas pelos Estados-Membros nos termos da presente diretiva, nomeadamente do seu artigo 8.º;

[...]

(62) [...] a criação nos Estados-Membros de autoridades de controlo que exerçam as suas funções com total independência constitui um elemento essencial da proteção das pessoas no que respeita ao tratamento de dados pessoais;

(63) [...] essas autoridades devem ser dotadas dos meios necessários para a realização das suas funções, incluindo poderes de inquérito ou de intervenção, especialmente em caso de reclamações, e poderes para intervir em processos judiciais; [...]»

4 Os artigos 1.º, 2.º, 25.º, 26.º, 28.º e 31.º da Diretiva 95/46 dispõem:

«*Artigo 1.º*

Objeto da diretiva

1. Os Estados-Membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

[...]

Artigo 2.º

Definições

Para efeitos da presente diretiva, entende-se por:

- a) ‘Dados pessoais’, qualquer informação relativa a uma pessoa singular identificada ou identificável (‘pessoa em causa’); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;
- b) ‘Tratamento de dados pessoais’ (‘tratamento’): qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

[...]

- d) ‘Responsável pelo tratamento’: a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinadas por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário;

[...]

Artigo 25.º

Princípios

1. Os Estados-Membros estabelecerão que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adotadas nos termos das outras disposições da presente diretiva, o país terceiro em questão assegurar um nível de proteção adequado.

2. A adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou setoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país.

3. Os Estados-Membros e a Comissão informar-se-ão mutuamente dos casos em que consideram que um país terceiro não assegura um nível de proteção adequado na aceção do n.º 2.

4. Sempre que a Comissão verificar, nos termos do procedimento previsto no n.º 2 do artigo 31.º, que um país terceiro não assegura um nível de proteção adequado na aceção do n.º 2 do presente artigo, os Estados-Membros tomarão as medidas necessárias para impedir qualquer transferência de dados de natureza idêntica para o país terceiro em causa.

5. Em momento oportuno, a Comissão encetará negociações com vista a obviar à situação resultante da constatação feita em aplicação do n.º 4.

6. A Comissão pode constatar, nos termos do procedimento previsto no n.º 2 do artigo 31.º, que um país terceiro assegura um nível de proteção adequado na aceção do n.º 2 do presente artigo em virtude da sua legislação interna ou dos seus compromissos internacionais, subscritos nomeadamente na sequência das negociações referidas no n.º 5, com vista à proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas.

Os Estados-Membros tomarão as medidas necessárias para dar cumprimento à decisão da Comissão.

Artigo 26.º

Derrogações

1. Em derrogação ao disposto no artigo 25.º e sob reserva de disposições em contrário do seu direito nacional em casos específicos, os Estados-Membros estabelecerão que a transferência de dados pessoais para um país terceiro que não assegure um nível de proteção adequado na aceção do n.º 2 do artigo 25.º poderá ter lugar desde que:

- a) A pessoa em causa tenha dado de forma inequívoca o seu consentimento à transferência; ou
- b) A transferência seja necessária para a execução de um contrato entre a pessoa em causa e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou
- c) A transferência seja necessária à execução ou celebração de um contrato celebrado ou a celebrar, no interesse da pessoa em causa, entre o responsável pelo tratamento e um terceiro; ou
- d) A transferência seja necessária ou legalmente exigida para a proteção de um interesse público importante, ou para a declaração, o exercício ou a defesa de um direito num processo judicial; ou
- e) A transferência seja necessária para proteger os interesses vitais da pessoa em causa; ou
- f) A transferência seja realizada a partir de um registo público que, nos termos de disposições legislativas ou regulamentares, se destine à informação do público e se encontre aberto à consulta pelo público em geral ou por qualquer pessoa que possa provar um interesse legítimo, desde que as condições estabelecidas na lei para a consulta sejam cumpridas no caso concreto.

2. Sem prejuízo do n.º 1, um Estado-Membro pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um país terceiro que não assegura um nível de proteção adequado na aceção do n.º 2 do artigo 25.º, desde que o responsável pelo tratamento apresente garantias suficientes de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respetivos direitos; essas garantias podem, designadamente, resultar de cláusulas contratuais adequadas.

3. O Estado-Membro informará a Comissão e os restantes Estados-Membros das autorizações que conceder nos termos do n.º 2.

Em caso de oposição, por um Estado-Membro ou pela Comissão devidamente justificada no que se refere à proteção da privacidade e dos direitos e liberdades fundamentais das pessoas, a Comissão adotará as medidas adequadas, nos termos do procedimento previsto no n.º 2 do artigo 31.º

Os Estados-Membros tomarão as medidas necessárias para dar cumprimento à decisão da Comissão.

[...]

Artigo 28.º

Autoridade de controlo

1. Cada Estado-Membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adotadas pelos Estados-Membros nos termos da presente diretiva.

Essas autoridades exercerão com total independência as funções que lhes forem atribuídas.

2. Cada Estado-Membro estabelecerá que as autoridades de controlo serão consultadas aquando da elaboração de medidas regulamentares ou administrativas relativas à proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais.

3. Cada autoridade do controlo disporá, nomeadamente:

- de poderes de inquérito, tais como o poder de aceder aos dados objeto de tratamento e de recolher todas as informações necessárias ao desempenho das suas funções de controlo,
- de poderes efetivos de intervenção, tais como, por exemplo, o de emitir pareceres previamente à [realização dos tratamentos, em conformidade com o artigo 20.º, e o de assegurar a publicação] adequada desses pareceres, o de ordenar o bloqueio, o apagamento ou a destruição dos dados, o de proibir temporária ou definitivamente o tratamento, o de dirigir uma advertência ou uma censura ao responsável pelo tratamento ou o de remeter a questão para os parlamentos nacionais ou para outras instituições políticas,
- do poder de intervir em processos judiciais no caso de violação das disposições nacionais adotadas nos termos da presente diretiva ou de levar essas infrações ao conhecimento das autoridades judiciais.

As decisões da autoridade de controlo que lesem interesses são passíveis de recurso jurisdicional.

4. Qualquer pessoa ou associação que a represente pode apresentar à autoridade de controlo um pedido para proteção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais. A pessoa em causa será informada do seguimento dado ao seu pedido.

Em particular, qualquer pessoa pode apresentar à autoridade de controlo um pedido de verificação da licitude de qualquer tratamento de dados, sempre que sejam aplicáveis as disposições nacionais adotadas por força do artigo 13.º O requerente será pelo menos informado da realização da verificação.

[...]

6. Cada autoridade de controlo é competente, independentemente do direito nacional aplicável ao tratamento em causa, para o exercício no território do seu Estado-Membro dos poderes que lhe foram atribuídos em conformidade com o n.º 3. Cada autoridade de controlo pode ser solicitada a exercer os seus poderes por uma autoridade de outro Estado-Membro.

[...]

Artigo 31.º

[...]

2. Sempre que se faça referência ao presente artigo, são aplicáveis os artigos 4.º e 7.º da Decisão 1999/468/CE [do Conselho, de 28 de junho de 1999, que fixa as regras de exercício das competências de execução atribuídas à Comissão (JO L 184, p. 23)], tendo-se em conta o disposto no seu artigo 8.º

[...]»

Decisão 2000/520

5 A Decisão 2000/520 foi adotada pela Comissão com base no artigo 25.º, n.º 6, da Diretiva 95/46.

6 Os considerandos 2, 5 e 8 desta decisão têm a seguinte redação:

«(2) A Comissão pode determinar se um país terceiro garante um nível de proteção adequado. Nesse caso podem ser transferidos dados pessoais a partir dos Estados-Membros sem que sejam necessárias garantias adicionais.

[...]

(5) O nível adequado de proteção da transferência de dados a partir da Comunidade Europeia para os Estados Unidos da América (EUA), nos termos da presente decisão, pode conseguir-se se as organizações derem cumprimento aos princípios da 'privacidade em porto seguro' relativos à proteção de dados pessoais transferidos de um Estado-Membro para os EUA (a seguir denominados 'os princípios') e às diretrizes das questões mais frequentes (a seguir designadas 'FAQ') que servem de guia no que respeita à aplicação dos princípios estabelecidos pelo Governo dos Estados Unidos em 21 de julho de 2000. Por outro lado, as organizações devem dar a conhecer publicamente as suas políticas em matéria de proteção da vida privada e ficar abrangidas pelo âmbito da competência da Federal Trade Commission (FTC) que, nos termos do artigo 5.º da lei relativa ao comércio federal (Section 5 of the Federal Trade Commission Act), garante a proibição dos atos ou as práticas desleais ou enganosas relativas ao comércio, ou de outros organismos públicos que efetivamente assegurem o respeito dos princípios aplicados em conformidade com as FAQ.

[...]

(8) Num interesse de transparência e para salvaguardar a capacidade de as autoridades competentes nos Estados-Membros assegurarem a proteção das pessoas no que diz respeito ao tratamento de dados pessoais, é necessário precisar na presente decisão as circunstâncias excecionais em que a suspensão de fluxos concretos de dados se pode justificar, apesar de verificado um nível de proteção adequado.»

7 Nos termos dos artigos 1.º a 4.º da Decisão 2000/520:

«*Artigo 1.º*

1. Nos termos do n.º 2 do artigo 25.º da Diretiva 95/46/CE, para efeitos de todas as atividades abrangidas pelo âmbito da diretiva, considera-se que os ‘princípios da privacidade em porto seguro’ (a seguir denominados ‘os princípios’) que figuram no anexo I da presente decisão, aplicados em conformidade com a orientação que proporcionam as questões mais frequentes (a seguir designadas ‘FAQ’), publicadas pelo Department of Commerce dos EUA, em 21 de julho de 2000 que figuram no anexo II da presente decisão, asseguram um nível adequado de proteção dos dados pessoais transferidos a partir da Comunidade Europeia para organizações estabelecidas nos Estados Unidos da América, tendo em conta os seguintes documentos emanados do Department of Commerce dos EUA:

- a) O resumo global de aplicação dos princípios de porto seguro que figura no anexo III;
- b) O memorando sobre danos por violação das regras de proteção da vida privada e autorizações explícitas previstas na lei dos EUA, que figura no anexo IV;
- c) O ofício da Federal Trade Commission que figura no anexo V;
- d) O ofício do Department of Transportation que figura no anexo VI.

2. No que respeita a cada transferência de dados:

- a) A organização destinatária dos dados comprometer-se-á clara e publicamente a cumprir os princípios aplicados em conformidade com as FAQ; e
- b) A referida organização fica sujeita aos poderes legais dos entes públicos administrativos norte-americanos referidos no anexo VII da presente decisão, com competência para investigar denúncias, tomar medidas contra práticas desleais e enganosas, assim como proceder à reparação de [danos sofridos por] pessoas singulares, independentemente do seu país de residência ou da sua nacionalidade, sempre que se verificar incumprimento dos princípios segundo as orientações das FAQ.

3. Considera-se que a organização que declarar a sua adesão aos princípios aplicados em conformidade com as FAQ cumpre o disposto no n.º 2, a partir da data em que comunicar ao Department of Commerce dos EUA ou ao seu representante, a divulgação do compromisso referido na alínea a) do n.º 2, bem como a identidade da entidade pública a que se refere a alínea b) do n.º 2.

Artigo 2.º

A presente decisão diz respeito tão só ao nível adequado de proteção previsto nos Estados Unidos da América nos termos dos princípios aplicados nos termos da[s] FAQ a fim de dar cumprimento ao disposto no n.º 1 do artigo 25.º da Diretiva 95/46/CE e não prejudica a aplicação de outras disposições da referida diretiva relativas ao tratamento de dados pessoais nos Estados-Membros e nomeadamente o seu artigo 4.º

Artigo 3.º

1. Sem prejuízo da competência para tomar medidas que garantam o cumprimento das disposições nacionais adotadas por força de outras disposições além das previstas no artigo 25.º da Diretiva 95/46/CE, as autoridades competentes dos Estados-Membros podem exercer as suas competências para suspender a transferência de dados para uma organização que tenha declarado a sua adesão aos princípios aplicados em conformidade com as FAQ, se isso se verificar necessário à proteção das pessoas no que diz respeito ao tratamento dos seus dados pessoais, nos casos seguintes:

- a) A entidade pública administrativa norte-americana referida no anexo VII da presente decisão, ou um mecanismo de recurso independente, nos termos da alínea a) do princípio de aplicação que figura no anexo I da presente decisão, determinou que a organização violou os princípios em conformidade com as FAQ; ou
- b) Existem fortes probabilidades para supor que os princípios não estão a ser respeitados. Há indícios de que o mecanismo de aplicação em causa não toma ou não tomará as medidas adequadas na altura necessária para resolver o caso em questão, que a continuação da transferência dos dados pode causar graves prejuízos às pessoas em causa e que as entidades competentes nos Estados-Membros envidaram esforços razoáveis, dadas as circunstâncias, para facultar à organização em causa a informação e oportunidade necessárias para responder.

A suspensão cessará assim que o respeito dos princípios aplicados em conformidade com as FAQ estiver assegurado e a autoridade competente em questão na Comunidade Europeia seja disso informada.

2. Os Estados-Membros devem informar imediatamente a Comissão da adoção de medidas nos termos do n.º 1.

3. Os Estados-Membros e a Comissão devem ainda manter-se mutuamente informados relativamente aos casos em que os organismos responsáveis pelo cumprimento dos princípios aplicados em conformidade com as FAQ nos Estados Unidos da América não garantam esse mesmo cumprimento.

4. Se a informação recolhida nos termos dos n.ºs 1 a 3 demonstrar que os organismos responsáveis pelo cumprimento dos princípios em conformidade com as FAQ nos Estados Unidos da América não desempenham eficazmente as suas funções, a Comissão deve informar o Department of Commerce norte-americano e, se necessário, apresentar um projeto de medidas, de acordo com o procedimento estabelecido no artigo 31.º da diretiva, para revogar ou suspender a presente decisão ou limitar o seu âmbito.

Artigo 4.º

1. A presente decisão pode ser adaptada em qualquer altura, à luz da experiência proporcionada pela sua aplicação e/ou se o nível de proteção proporcionado pelos princípios e pelas FAQ for considerado insuficiente pela lei norte-americana. Em qualquer caso, a Comissão deve apreciar a aplicação da presente decisão com base na informação disponível, três anos após a sua notificação aos Estados-Membros, e informar o comité estabelecido pelo artigo 31.º da Diretiva 95/46/CE de todas as conclusões pertinentes e, nomeadamente, de todas as provas que possam afetar a apreciação da adequação do nível de proteção do disposto no artigo 1.º da presente decisão, nos termos do artigo 25.º da diretiva, e de todas as provas de aplicação discriminatória da decisão.

2. A Comissão apresentará, se necessário, projetos de medidas de acordo com o previsto no artigo 31.º da diretiva.»

8 O anexo I da Decisão 2000/520 tem a seguinte redação:

«Princípios de ‘porto seguro’ (proteção da vida privada) emitidos pelo Department of Commerce dos EUA em 21 de julho de 2000 [...] [...] o Department of Commerce formula o presente documento e as FAQ, questões mais frequentes (os princípios), nos termos da sua autoridade legal para incentivar, promover e desenvolver o comércio internacional. Os princípios foram desenvolvidos com base em consultas ao setor e ao público em geral para facilitar as relações comerciais e as transações entre os Estados Unidos e a União Europeia. Destinam-se a ser utilizados exclusivamente por organizações dos EUA que recebam dados pessoais da União Europeia para efeitos de reconhecimento como ‘porto seguro’ e para a presunção de ‘adequação’ implicada nesse processo. Visto que estes princípios foram concebidos com aquele objetivo específico, a sua adoção para outros fins pode revelar-se imprópria. [...] A decisão de preencher os requisitos de ‘porto seguro’ é inteiramente voluntária e as organizações podem preencher os requisitos de ‘porto seguro’ de várias formas. [...] A adesão a estes princípios pode ser limitada: a) na medida necessária para observar requisitos de segurança nacional, interesse público ou [cumprimento da lei], b) por legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores [prosseguidos] por essa autorização, ou c) por exceção ou derrogação prevista na diretiva ou nas normas de direito interno dos Estados-Membros, desde que a aplicação das referidas exceções ou derrogações ocorra em contextos comparáveis. Para que se possa melhorar a proteção da vida privada, as organizações deverão envidar esforços no sentido de aplicar estes princípios de forma integral e transparente, incluindo a indicação das respetivas políticas de proteção da vida privada, sempre que as exceções aos princípios permitidas pela alínea b) *supra* se apliquem regularmente. Pela mesma razão, quando a escolha for permitida pelos princípios e/ou pela legislação norte-americana, as organizações deverão optar pelo nível de proteção mais elevado possível. [...]»

9 O anexo II da Decisão 2000/520 tem a seguinte redação:

«Questões mais frequentes (FAQ)

[...] FAQ 6 — Autocertificação

Q: De que modo uma organização autocertifica a sua adesão aos princípios de ‘porto seguro’?

R: Os benefícios decorrentes da adesão ao ‘porto seguro’ vigoram a partir da data em que cada organização autocertifica junto do Department of Commerce (ou do respetivo representante) a sua adesão aos princípios, em conformidade com as orientações que a seguir se especificam.

Para proceder à autocertificação de adesão aos princípios de ‘porto seguro’, as organizações poderão apresentar ao Department of Commerce (ou a um seu representante) uma carta assinada por um dos responsáveis da organização aderente ao ‘porto seguro’, em nome desta, contendo, no mínimo, a seguinte informação:

- 1) Designação da organização, endereço postal e de correio eletrónico, números de telefone e fax;
- 2) Descrição das atividades da organização em matéria de informação pessoal recebida da UE; e
- 3) Descrição da política da organização em matéria de proteção da vida privada no que diz respeito a essa informação pessoal, incluindo: a) o local onde pode ser consultada pelo público, b) a sua data de aplicação, c) o nome do gabinete de contacto para a apresentação de queixas, pedidos de acesso ou quaisquer outros assuntos relacionados com os princípios de

‘porto seguro’, d) os organismos oficiais concretos com competência para deliberar sobre quaisquer queixas contra a organização em matéria de práticas desleais ou desonestas e violações das leis ou normas que regulamentam a proteção da vida privada (e que se encontram referidos no anexo dos princípios), e) a designação de qualquer programa relativo à proteção da vida privada em que a organização participe, f) o método de verificação (por exemplo, interno ou por terceiros) [...] e g) o mecanismo de recurso independente que possa ser utilizado para investigar as queixas por resolver.

Se a organização desejar que a sua adesão aos princípios de ‘porto seguro’ abranja também a informação sobre recursos humanos transferida da UE para ser utilizada num contexto de relações laborais pode fazê-lo, desde que exista um organismo oficial com competência para conhecer de queixas contra a referida organização, em matéria de informações sobre recursos humanos, referido na lista anexa aos princípios. [...]

O Department of Commerce (ou o seu representante) terá uma lista de todas as organizações que autocertificarem a sua adesão ao ‘porto seguro’, garantindo desta forma os benefícios daí decorrentes, que atualizará com base nas cartas anuais e notificações que receba, de acordo com a FAQ 11. [...]

[...] FAQ 11 — Resolução de litígios e aplicação

Q: *Como deverão ser implementados os requisitos de resolução de litígios previstos no princípio de aplicação e como deverá ser tratado o problema de uma organização que persista em não cumprir os princípios?*

R: O princípio de aplicação estabelece os requisitos observados pelos mecanismos de aplicação dos princípios de ‘porto seguro’. Como cumprir os requisitos do ponto b) do princípio consta da FAQ sobre verificação (FAQ 7). A presente FAQ (FAQ 11) aborda os pontos a) e c) que exigem mecanismos de recurso independentes. Esses mecanismos podem assumir formas diferentes, mas todos devem cumprir os requisitos do princípio de aplicação. As organizações podem cumprir os requisitos das seguintes maneiras: 1. aplicando programas do setor privado de proteção da privacidade que respeitem os princípios de ‘porto seguro’ nas suas regras e que incluam mecanismos de aplicação efetivamente eficazes do tipo descrito no princípio de aplicação, 2. obedecendo às regras estabelecidas por entidades de controlo legal ou regulamentar que prevejam o tratamento de queixas individuais e resolução de litígios, ou 3. comprometendo-se a cooperar com as autoridades de proteção dos dados da Comunidade Europeia ou os seus representantes autorizados. Esta lista pretende ser ilustrativa sem ser limitativa. O setor privado pode criar outros mecanismos de aplicação, desde que os mesmos cumpram o estabelecido no princípio de aplicação e nas FAQ. É de referir que os requisitos do princípio de aplicação complementam o requisito, estabelecido no n.º 3 da introdução aos princípios, segundo o qual as iniciativas de autorregulamentação devem ser vinculativas, em conformidade com o artigo 5.º da lei relativa ao comércio federal (Federal Trade Commission Act) ou regulamentação semelhante.

Mecanismos de recurso

Antes de mais, as pessoas devem ser encorajadas a apresentar queixas que possam ter à organização em causa, antes de recorrerem a mecanismos de recurso independentes. [...]

[...]

Atividade da FTC

A FTC (Federal Trade Commission) comprometeu-se a examinar prioritariamente as queixas trazidas por organizações privadas de autorregulamentação, como BBBOnline e TRUSTe, e as dos Estados-Membros da UE em matéria de incumprimento dos princípios de ‘porto seguro’, para determinar se há violação do artigo 5.º da lei relativa à Comissão reguladora do comércio federal (Section 5 of the Federal Trade Commission Act), que proíbe os atos ou as práticas desleais ou enganosas. [...] [...]»

10 Nos termos do anexo IV da Decisão 2000/520:

«[D]anos por violação da privacidade, autorizações legais e fusões e aquisições nos termos da] legislação dos EUA

O presente documento responde ao pedido apresentado pela Comissão Europeia, de clarificação da legislação dos Estados Unidos da América em matéria de a) queixas por quebra da privacidade, b) ‘autorizações explícitas’ na legislação dos EUA no que respeita ao uso de informação pessoal de forma incoerente com os princípios de ‘porto seguro’, e c) efeitos das fusões e aquisições nos compromissos decorrentes do ‘porto seguro’.

[...]

B. Autorizações legais explícitas Os princípios de ‘porto seguro’ contêm exceções nos casos em que uma lei, um regulamento ou a jurisprudência criem ‘obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores avançados por essa autorização’. Claramente, sempre que a legislação norte-americana impõe uma obrigação contraditória, as organizações norte-americanas, aderentes ou não ao ‘porto seguro’ têm que aplicar a lei. Quanto às autorizações explícitas, enquanto os princípios de ‘porto seguro’ se destinam a colmatar as diferenças entre os regimes europeus e norte-americanos de proteção da vida privada, devemos respeitar as prerrogativas legislativas dos nossos legisladores eleitos. A exceção limitada ao respeito rigoroso dos princípios de ‘porto seguro’ procura equilibrar os interesses legítimos de ambas as partes. A exceção limita-se a casos em que existe autorização explícita. Assim, em último caso, a lei relevante, o regulamento ou a decisão do tribunal devem autorizar especificamente essa conduta particular por parte das organizações do ‘porto seguro’. Por outras palavras, a exceção não se aplica quando a lei for omissa. Além disso, a exceção aplicar-se-á apenas se a autorização específica for contraditória com os princípios de ‘porto seguro’. Mesmo então, a exceção não deverá ultrapassar o ‘necessário para respeitar os legítimos interesses superiores avançados por essa autorização’. Como exemplo, pode dizer-se que quando a lei autoriza simplesmente uma empresa a fornecer informação pessoal às entidades públicas, a exceção não se aplica. Em contrapartida, quando a lei autorizar especificamente uma empresa a fornecer informação pessoal a agências governamentais sem o consentimento da pessoa, isto constituirá uma ‘autorização explícita’ para agir de forma contraditória com os princípios do ‘porto seguro’. Alternativamente, as exceções específicas às exigências afirmativas para fornecer aviso e obter consentimento seriam abrangidas pelo âmbito da exceção (uma vez que seriam equivalentes a uma autorização específica para divulgar informação sem aviso nem consentimento). Por exemplo, uma norma que autorize os médicos a divulgar aos serviços de saúde os *dossiers* dos seus pacientes, sem o consentimento prévio destes últimos, poderia permitir uma exceção aos princípios de aviso e escolha. Tal autorização não permitiria a um médico facultar os mesmos *dossiers* a organizações de saúde ou laboratórios farmacêuticos, não abrangidos pelo âmbito dos objetivos autorizados pela lei e, assim, não podem ser considerados exceção [...]. A autorização em

questão pode ser uma autorização ‘única’ para proceder de determinada forma com informação pessoal, mas, como ilustram os exemplos seguintes, é provável que seja uma exceção a uma lei mais abrangente que regulamente a recolha, uso e divulgação de informação pessoal. [...]»

Comunicação COM(2013) 846 final

- 11 Em 27 de novembro de 2013, a Comissão adotou a Comunicação ao Parlamento Europeu e ao Conselho, intitulada «Restabelecer a confiança nos fluxos de dados entre a UE e os EUA» [COM(2013) 846 final, a seguir «Comunicação COM(2013) 846 final»]. Esta comunicação era acompanhada de um relatório, igualmente com data de 27 de novembro de 2013, que continha as «conclusões dos copresidentes da UE do grupo de trabalho *ad hoc* União Europeia — Estados Unidos sobre proteção de dados pessoais» («Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection»). Este relatório tinha sido elaborado, como indica o seu n.º 1, em cooperação com os Estados Unidos da América na sequência da revelação da existência, neste país, de vários programas de vigilância que incluíam a recolha e o tratamento em grande escala de dados pessoais. O referido relatório continha, nomeadamente, uma análise detalhada da ordem jurídica dos Estados Unidos no que respeita, em particular, às bases legais que autorizam a existência dos programas de vigilância bem como a recolha e o tratamento de dados pessoais por parte das autoridades americanas.
- 12 No ponto 1 da Comunicação COM(2013) 846 final, a Comissão precisou que «[a]s trocas comerciais são abordadas na Decisão [2000/520]», acrescentado que esta decisão «constitui a base jurídica das transferências de dados pessoais da UE para as empresas sediadas nos EUA que tenham subscrito os princípios de privacidade do sistema ‘porto seguro’» Além disso, neste mesmo ponto 1, Comissão destacou a importância cada vez maior dos fluxos de dados pessoais, associada, nomeadamente, ao desenvolvimento da economia digital, tendo este, com efeito, «ger[ado] um crescimento exponencial da quantidade, da qualidade, da diversidade e da natureza das atividades de tratamento de dados».
- 13 No ponto 2 dessa comunicação, a Comissão observou que «aumentou a preocupação com o nível de proteção dos dados pessoais dos cidadãos da UE que são transferidos para os EUA através [do sistema ‘porto seguro’]» e que «[a] adesão voluntária e o seu caráter declaratório fizeram com que a atenção se centrasse na transparência e na aplicação efetiva do sistema».
- 14 A Comissão indicou, além disso, neste mesmo ponto 2, que «[o]s dados pessoais dos cidadãos da UE enviados para os EUA através do sistema [‘porto seguro’] podem ser acedidos e posteriormente tratados pelas autoridades dos EUA de uma forma que é incompatível com os motivos pelos quais esses dados foram originalmente recolhidos na UE e com os fins para os quais foram transferidos para os EUA» e que «[a] maioria das empresas de Internet norte-americanas mais diretamente envolvidas n[os] programas [de vigilância] são certificadas ao abrigo do sistema ‘porto seguro’».
- 15 No ponto 3.2 da Comunicação COM(2013) 846 final, a Comissão salientou a existência de algumas deficiências relativas à execução da Decisão 2000/520. Nele indica, por um lado, que há empresas americanas certificadas que não respeitavam os princípios previstos no artigo 1.º, n.º 1, da Decisão 2000/520 (a seguir «princípios de porto seguro») e que deviam ser introduzidas melhorias nesta decisão quanto «[à]s deficiências estruturais relacionadas com a transparência e o cumprimento das regras do sistema, os princípios materiais ‘porto seguro’ e o recurso à derrogação por motivos de segurança nacional». Por outro lado, observou que o «‘porto seguro’ funciona igualmente como um canal para transferir dados pessoais dos cidadãos da UE para os EUA pelas empresas que estão obrigadas a fornecer dados aos serviços de informações norte-americanos no âmbito dos programas de recolha de informações dos EUA».

- 16 A Comissão concluiu, neste mesmo ponto 3.2, que, embora, «[d]adas as deficiências identificadas, não se pode continuar a aplicar o sistema como tem vindo a ser aplicado até à data, [...] a sua revogação afetaria negativamente os interesses das empresas, tanto da UE como dos EUA, que são membros do sistema. Por fim, sempre no referido ponto 3.2, a Comissão acrescentou que iria «encetar urgentemente um diálogo com as autoridades dos EUA para debater as deficiências identificadas».

Comunicação COM(2013) 847 final

- 17 No mesmo dia, 27 de novembro de 2013, a Comissão adotou a Comunicação ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE [COM(2013) 847 final, a seguir «Comunicação COM(2013) 847 final»]. Como resulta do seu ponto 1, esta comunicação baseava-se, nomeadamente, nas informações recebidas pelo grupo de trabalho *ad hoc* União Europeia — Estados Unidos, e inscrevia-se na sequência de dois relatórios de avaliação da Comissão publicados, respetivamente, em 2002 e em 2004.
- 18 O ponto 1 desta comunicação precisa que o funcionamento da Decisão 2000/520 «[se baseia] em compromissos, bem como na autocertificação das empresas participantes» e acrescenta que «[e]mbora a assinatura destes acordos seja voluntária, as regras são vinculativas».
- 19 Além disso, decorre do ponto 2.2 da Comunicação COM(2013) 847 final que, em 26 de setembro de 2013, estavam certificadas 3 246 empresas, pertencentes a um grande número de setores da indústria e dos serviços. Estas empresas forneciam, principalmente, serviços no mercado interno da União, em particular no setor da Internet, e parte delas eram empresas da União com filiais nos Estados Unidos. Algumas destas empresas tratavam os dados dos seus trabalhadores na Europa, que eram transferidos para os EUA para efeitos de gestão de recursos humanos.
- 20 Neste mesmo ponto 2.2, a Comissão salientou que «a falta de transparência ou insuficiências a nível da aplicação por parte dos EUA acarreta[va]m a transferência da responsabilidade para as autoridades europeias responsáveis pela proteção de dados, bem como para as empresas que utilizam o sistema».
- 21 Resulta, nomeadamente, dos pontos 3 a 5 e 8 da Comunicação COM(2013) 847 final que, na prática, um número considerável de empresas certificadas não respeitavam, ou não respeitavam na íntegra, os princípios de porto seguro.
- 22 Além disso, no ponto 7 dessa comunicação, a Comissão indica que «todas as empresas que participam no Programa PRISM [programa de recolha de informações em grande escala], que permite às autoridades americanas ter acesso a dados armazenados e tratados nos EUA, parecem estar certificadas no âmbito do sistema de ‘porto seguro’» e que este sistema «passou, pois, a ser uma das vias através da qual os serviços de informações americanos têm acesso à recolha de dados pessoais inicialmente tratados na UE». A este respeito, a Comissão declarou, no ponto 7.1 da referida comunicação, que «uma série de bases jurídicas previstas pela legislação americana permitem recolher e tratar em grande escala dados pessoais, que são armazenados ou tratados por empresas estabelecidas nos EUA» e que «[c]omo se trata de programas de grande envergadura, é possível que os dados transferidos no âmbito do sistema de ‘porto seguro’ sejam acessíveis às autoridades americanas e sejam por estas tratados para além do estritamente necessário e proporcional em relação à proteção da segurança nacional, como previsto na derrogação enunciada na Decisão [2000/520]».
- 23 No ponto 7.2 da Comunicação COM(2013) 847 final, intitulado «Limitações e possibilidades de recurso», a Comissão salientou que «são sobretudo os cidadãos dos EUA ou os residentes legais que beneficiam das salvaguardas fornecidas ao abrigo da legislação americana» e que «[a]lém disso, não existe qualquer possibilidade de os titulares de dados da UE ou dos EUA obterem acesso ou

solicitarem a retificação ou a supressão dos dados, ou apresentarem um recurso administrativo ou judicial caso, no âmbito de programas de vigilância dos EUA, os seus dados pessoais sejam recolhidos e tratados posteriormente».

- 24 Segundo o ponto 8 da Comunicação COM(2013) 847 final, encontravam-se entre as empresas certificadas «as empresas da Internet como a Google, Facebook, Microsoft, Apple e Yahoo», que tinham estas «centenas de milhões de clientes na Europa» e transferiam dados pessoais para os EUA a fim de serem tratados.
- 25 A Comissão concluiu, neste mesmo n.º 8, que «o acesso em grande escala pelos serviços de informações a dados transferidos para os EUA por empresas certificadas participantes no sistema de ‘porto seguro’ levanta novas questões graves sobre a continuidade dos direitos dos cidadãos europeus em matéria de proteção de dados quando os seus dados pessoais são transferidos para os EUA».

Litígio no processo principal e questões prejudiciais

- 26 M. Schrems, cidadão austríaco residente na Áustria, é utilizador da rede social Facebook (a seguir «Facebook») desde 2008.
- 27 Todas as pessoas que residam no território da União e pretendam utilizar o Facebook são obrigadas, no momento da sua inscrição, a celebrar um contrato com a Facebook Ireland, filial da Facebook Inc., com sede nos Estados Unidos. Os dados pessoais dos utilizadores do Facebook residentes no território da União são, no todo ou em parte, transferidos para servidores pertencentes à Facebook Inc., situados em território dos Estados Unidos, onde são objeto de tratamento.
- 28 Em 25 de junho de 2013, M. Schrems apresentou ao Commissioner uma queixa em que lhe pedia, em substância, que exercesse as suas competências estatutárias proibindo a Facebook Ireland de transferir os seus dados pessoais para os Estados Unidos. Alegava que o direito e as práticas em vigor neste país não asseguravam uma proteção suficiente dos dados pessoais conservados no seu território contra as atividades de vigilância aí exercidas pelas autoridades públicas. M. Schrems referia-se, a este respeito, às revelações feitas por Edward Snowden sobre as atividades dos serviços de informação dos Estados Unidos, nomeadamente as da National Security Agency (Agência Nacional de Segurança) (a seguir «NSA»).
- 29 Por entender que não estava obrigado a investigar os factos denunciados por M. Schrems na sua queixa, o Commissioner arquivou-a por falta de fundamento. Com efeito, considerou que não havia provas de que a NSA tivesse acedido aos dados pessoais do interessado. Acrescentou que as críticas suscitadas por M. Schrems na sua queixa não podiam ser utilmente invocadas, dado que qualquer questão relativa ao carácter adequado da proteção dos dados pessoais nos Estados Unidos devia ser decidida em conformidade com a Decisão 2000/520 e que, nesta decisão, a Comissão tinha constatado que os Estados Unidos asseguravam um nível de proteção adequado.
- 30 M. Schrems interpôs recurso para a High Court (Supremo Tribunal de Justiça) da decisão em causa no processo principal. Depois de ter analisado as provas apresentadas pelas partes no processo principal, aquele órgão jurisdicional declarou que a vigilância eletrónica e a interceção de dados pessoais transferidos da União para os Estados Unidos respondiam a finalidades necessárias e indispensáveis ao interesse público. Todavia, o referido órgão jurisdicional acrescentou que as revelações de E. Snowden tinham demonstrado que a NSA e outros órgãos federais haviam cometido «excessos consideráveis».
- 31 Ora, segundo esse mesmo órgão jurisdicional, os cidadãos da União não dispõem de nenhum direito efetivo a ser ouvidos. A supervisão das ações dos serviços de informações é feita através de procedimentos secretos e não contraditórios. Após a transferência de dados pessoais para os Estados

Unidos, a NSA e outros órgãos federais, como o Federal Bureau of Investigation (FBI), podem aceder a tais dados no âmbito da vigilância e das interceções indiscriminadas a que procedem em grande escala.

- 32 A High Court (Supremo Tribunal de Justiça) declarou que o direito irlandês proíbe a transferência de dados pessoais para fora do território nacional, salvo se o país terceiro em questão assegurar um nível adequado de proteção da vida privada bem como dos direitos e liberdades fundamentais. A importância dos direitos ao respeito da vida privada e à inviolabilidade do domicílio, garantidos pela Constituição irlandesa, exige que qualquer ingerência nestes direitos seja proporcionada e respeite os requisitos previstos pela lei.
- 33 Ora, o acesso massivo e indiscriminado a dados pessoais é, evidentemente, contrário ao princípio da proporcionalidade e aos valores fundamentais protegidos pela Constituição irlandesa. Para as interceções das comunicações eletrónicas serem consideradas conformes a essa Constituição, é necessário apresentar provas de que tais interceções têm caráter seletivo, de que a vigilância de certas pessoas ou de certos grupos de pessoas se justifica objetivamente no interesse da segurança nacional ou do combate à criminalidade, e de que existem garantias adequadas e verificáveis. Assim, segundo a High Court (Supremo Tribunal de Justiça), se o processo principal fosse julgado apenas com base no direito irlandês, haveria então que concluir que, atendendo à existência de uma dúvida séria sobre a questão de saber se os Estados Unidos da América asseguram um nível de proteção adequado dos dados pessoais, o Commissioner devia ter procedido a uma investigação dos factos denunciados por M. Schrems na sua queixa, e que não teve razão ao arquivá-la.
- 34 Todavia, a High Court (Supremo Tribunal de Justiça) considera que este processo respeita à aplicação do direito da União na aceção do artigo 51.º da Carta, pelo que a legalidade da decisão em causa no processo principal deve ser apreciada à luz do direito da União. Ora, segundo esse órgão jurisdicional, a Decisão 2000/520 não satisfaz os requisitos que decorrem tanto dos artigos 7.º e 8.º da Carta como dos princípios estabelecidos pelo Tribunal de Justiça no acórdão Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238). O direito ao respeito da vida privada, garantido pelo artigo 7.º da Carta e pelos valores fundamentais comuns às tradições constitucionais dos Estados-Membros, ficaria privado do seu alcance se se permitisse que os poderes públicos acessem às comunicações eletrónicas de forma aleatória e generalizada, sem nenhuma justificação objetiva baseada em considerações de segurança nacional ou de prevenção da criminalidade, associadas especificamente aos indivíduos em causa, e sem que essas práticas fossem rodeadas de garantias adequadas e verificáveis.
- 35 A High Court (Supremo Tribunal de Justiça) observa, além disso, que, no seu recurso, M. Schrems questiona, na realidade, a legalidade do regime do «porto seguro» estabelecido pela Decisão 2000/520 e do qual procede a decisão em causa no processo principal. Assim, embora M. Schrems não tenha contestado formalmente a validade da Diretiva 95/46 nem da Decisão 2000/520, coloca-se a questão, segundo aquele órgão jurisdicional, de saber se, nos termos do artigo 25.º, n.º 6, desta diretiva, o Commissioner estava vinculado pela constatação efetuada pela Comissão na decisão, segundo a qual os Estados Unidos da América asseguram um nível de proteção adequado, ou se o artigo 8.º da Carta autorizava o Commissioner a afastar-se, sendo caso disso, dessa constatação.
- 36 Foi nestas condições que a High Court (Supremo Tribunal de Justiça) decidiu suspender a instância e submeter ao Tribunal de Justiça as questões prejudiciais seguintes:
- «1) Tendo em conta os artigos 7.º, 8.º e 47.º da Carta [...] e sem prejuízo das disposições do artigo 25.º, n.º 6, da Diretiva 95/46, o [Commissioner] encarregad[o] de aplicar a legislação sobre a proteção de dados pessoais no âmbito da análise de uma queixa segundo a qual o direito e as práticas de um país terceiro (neste caso, os Estados Unidos da América) para o qual são enviados dados pessoais não oferecem proteção adequada, está vinculado em termos absolutos pela constatação em sentido contrário da União, contida na Decisão 2000/520?

- 2) Em alternativa, pode e/ou deve proceder à sua própria investigação sobre a matéria, à luz dos últimos desenvolvimentos de facto ocorridos desde a primeira publicação da decisão da Comissão?»

Quanto às questões prejudiciais

- 37 Através das suas questões prejudiciais, que devem ser examinadas conjuntamente, o órgão jurisdicional de reenvio pergunta, em substância, se, e em que medida, o artigo 25.º, n.º 6, da Diretiva 95/46, lido à luz dos artigos 7.º, 8.º e 47.º da Carta, deve ser interpretado no sentido de que uma decisão adotada nos termos desta disposição, como a Decisão 2000/520, através da qual a Comissão constata que um país terceiro assegura um nível de proteção adequado, obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do artigo 28.º desta diretiva, examine o pedido de uma pessoa, relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado.

Quanto aos poderes das autoridades nacionais de controlo, na aceção do artigo 28.º da Diretiva 95/46, perante uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, desta diretiva

- 38 Importa recordar, a título preliminar, que as disposições da Diretiva 95/46, na medida em que regulam o tratamento de dados pessoais suscetível de pôr em causa as liberdades fundamentais, em especial o direito à vida privada, devem necessariamente ser interpretadas à luz dos direitos fundamentais garantidos pela Carta (v. acórdãos Österreichischer Rundfunk e o., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, n.º 68; Google Spain e Google, C-131/12, EU:C:2014:317, n.º 68; e Ryneš, C-212/13, EU:C:2014:2428, n.º 29).
- 39 Resulta do artigo 1.º, bem como dos considerandos 2 e 10 da Diretiva 95/46, que esta visa assegurar não só uma proteção eficaz e completa das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente o direito fundamental à vida privada, no que diz respeito ao tratamento de dados pessoais, como também um elevado nível de proteção dessas liberdades e desses direitos fundamentais. A importância tanto do direito fundamental à vida privada, garantido pelo artigo 7.º da Carta, como do direito fundamental à proteção dos dados pessoais, garantido pelo seu artigo 8.º é, além disso, sublinhada na jurisprudência do Tribunal de Justiça (v. acórdãos Rijkeboer, C-553/07, EU:C:2009:293, n.º 47; Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 53; e Google Spain e Google, C-131/12, EU:C:2014:317, n.ºs 53, 66 e 74 e jurisprudência aí referida).
- 40 No que respeita aos poderes de que dispõem as autoridades de controlo nacionais quanto às transferências de dados pessoais para países terceiros, importa salientar que o artigo 28.º, n.º 1, da Diretiva 95/46 impõe aos Estados-Membros que instituam uma ou mais autoridades públicas encarregadas de fiscalizar, com total independência, o cumprimento das regras da União relativas à proteção das pessoas singulares no que diz respeito ao tratamento de tais dados. Esta exigência resulta igualmente do direito primário da União, nomeadamente do artigo 8.º, n.º 3, da Carta e do artigo 16.º, n.º 2, TFUE (v., neste sentido, acórdãos Comissão/Áustria, C-614/10, EU:C:2012:631, n.º 36, e Comissão/Hungria, C-288/12, EU:C:2014:237, n.º 47).
- 41 A garantia de independência das autoridades nacionais de controlo visa assegurar a eficácia e a fiabilidade do controlo do cumprimento 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. Essa exigência foi estabelecida para reforçar a proteção das pessoas e dos organismos abrangidos pelas decisões dessas autoridades. A instituição, nos Estados-Membros, de autoridades de controlo independentes constitui, portanto, como salienta o considerando 62 da Diretiva 95/46, um

elemento essencial do respeito da proteção das pessoas relativamente ao tratamento de dados pessoais (v. acórdãos Comissão/Alemanha, C-518/07, EU:C:2010:125, n.º 25, e Comissão/Hungria, C-288/12, EU:C:2014:237, n.º 48 e jurisprudência aí referida).

- 42 Para garantir essa proteção, as autoridades de controlo devem, nomeadamente, assegurar um justo equilíbrio entre, por um lado, o respeito do direito fundamental à vida privada e, por outro, os interesses que regem uma livre circulação de dados pessoais (v., neste sentido, acórdãos Comissão/Alemanha, C-518/07, EU:C:2010:125, n.º 24, e Comissão/Hungria, C-288/12, EU:C:2014:237, n.º 51).
- 43 Para este efeito, essas autoridades dispõem de um amplo leque de poderes, enumerados de forma não exaustiva no artigo 28.º, n.º 3, da Diretiva 95/46, que constituem os meios necessários para a realização das suas funções, como sublinha o considerando 63 desta diretiva. 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.
- 44 É certo que decorre do artigo 28.º, 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.º, relativamente aos tratamentos de tais dados efetuados no território de um país terceiro.
- 45 Porém, a transferência de dados pessoais de um Estado-Membro para um país terceiro constitui, enquanto tal, um tratamento de dados pessoais na aceção do artigo 2.º, alínea b), da Diretiva 95/46 (v., neste sentido, acórdão Parlamento/Conselho e Comissão, C-317/04 e C-318/04, EU:C:2006:346, n.º 56), efetuado no território de um Estado-Membro. Com efeito, esta disposição define o «tratamento de dados pessoais» como «qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados» e indica, a título de exemplo, a «comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição».
- 46 O considerando 60 da Diretiva 95/46 precisa que as transferências de dados pessoais para países terceiros só podem ser efetuadas no pleno respeito das disposições adotadas pelos Estados-Membros nos termos dessa diretiva. Quanto a este aspeto, o capítulo IV da referida diretiva, no qual se inserem os seus artigos 25.º e 26.º, instituiu um regime que visa assegurar o controlo, pelos Estados-Membros, das transferências de dados pessoais para os países terceiros. Este regime é complementar do regime geral instituído pelo capítulo II da mesma diretiva, que prevê as condições gerais da licitude do tratamento de dados pessoais (v., neste sentido, acórdão Lindqvist, C-101/01, EU:C:2003:596, n.º 63).
- 47 Uma vez que as autoridades nacionais de controlo estão encarregadas, nos termos do artigo 8.º, n.º 3, da Carta e do artigo 28.º da Diretiva 95/46, da fiscalização 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, portanto, competência para verificar se uma transferência de dados pessoais do Estado-Membro dessa autoridade para um país terceiro respeita os requisitos estabelecidos pela Diretiva 95/46.
- 48 Embora reconheça, no seu considerando 56, que as transferências de dados pessoais dos Estados-Membros para países terceiros são necessárias para o desenvolvimento do comércio internacional, a Diretiva 95/46 estabelece como princípio, a saber, no seu artigo 25.º, n.º 1, que tais transferências só podem ter lugar se esses países terceiros assegurarem um nível de proteção adequado.
- 49 Além disso, o considerando 57 da referida diretiva precisa que as transferências de dados pessoais para países terceiros que não assegurem um nível de proteção adequado devem ser proibidas.

- 50 Para controlar as transferências de dados pessoais para os países terceiros em função do nível de proteção que lhes é conferido em cada um desses países, o artigo 25.º da diretiva 95/46 impõe uma série de obrigações aos Estados-Membros e à Comissão. Resulta deste artigo, nomeadamente, que a constatação de que um país terceiro assegura ou não um nível de proteção adequado pode, como o advogado-geral observou no n.º 86 das suas conclusões, ser feita quer pelos Estados-Membros quer pela Comissão.
- 51 A Comissão pode, com base no artigo 25.º, n.º 6, da Diretiva 95/46, adotar uma decisão que constate que um país terceiro assegura um nível de proteção adequado. Nos termos do segundo parágrafo desta disposição, tal decisão tem como destinatários os Estados-Membros, os quais devem tomar as medidas necessárias para lhe dar cumprimento. Por força do artigo 288.º, quarto parágrafo, TFUE, a referida decisão possui caráter obrigatório para todos os Estados-Membros destinatários e impõe-se, portanto, a todos os seus órgãos (v., neste sentido, acórdãos *Albako Margarinefabrik*, 249/85, EU:C:1987:245, n.º 17, e *Mediaset*, C-69/13, EU:C:2014:71, n.º 23), na medida em que tem por efeito autorizar transferências de dados pessoais dos Estados-Membros para o país terceiro visado pela mesma.
- 52 Assim, enquanto a decisão da Comissão não for declarada inválida pelo Tribunal de Justiça, os Estados-Membros e os seus órgãos, entre os quais se encontram as autoridades de controlo independentes, não podem adotar medidas contrárias a essa decisão, tais como atos destinados a constatar, com efeitos vinculativos, que o país terceiro visado pela referida decisão não assegura um nível de proteção adequado. Com efeito, os atos das instituições da União gozam, em princípio, de uma presunção de legalidade e produzem, portanto, efeitos jurídicos enquanto não forem revogados, anulados no âmbito de um recurso de anulação ou declarados inválidos na sequência de um pedido prejudicial ou de uma questão prévia de ilegalidade (acórdão *Comissão/Grecia*, C-475/01, EU:C:2004:585, n.º 18 e jurisprudência aí referida).
- 53 Todavia, uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, da Diretiva 95/46, como a Decisão 2000/520, não pode impedir as pessoas cujos dados pessoais tenham sido ou possam ser transferidos para um país terceiro de apresentarem às autoridades nacionais de controlo um pedido, nos termos do artigo 28.º, n.º 4, desta diretiva, relativo à proteção dos seus direitos e liberdades no que diz respeito ao tratamento desses dados. De igual modo, como o advogado-geral salientou, nomeadamente, nos n.ºs 61, 93 e 116 das suas conclusões, uma decisão desta natureza não pode suprimir nem reduzir os poderes expressamente reconhecidos às autoridades nacionais de controlo pelo artigo 8.º, n.º 3, da Carta bem como pelo artigo 28.º da referida diretiva.
- 54 Nem o artigo 8.º, n.º 3, da Carta nem o artigo 28.º da Diretiva 95/46 excluem do âmbito da competência das autoridades nacionais de controlo a fiscalização das transferências de dados pessoais para países terceiros que tenham sido objeto de uma decisão da Comissão nos termos do artigo 25.º, n.º 6, desta diretiva.
- 55 Em particular, o artigo 28.º, n.º 4, primeiro parágrafo, da Diretiva 95/46, que dispõe que pode ser apresentado às autoridades nacionais de controlo, por «[q]ualquer pessoa [...] um pedido para proteção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais», não prevê nenhuma exceção neste âmbito no caso de a Comissão ter adotado uma decisão nos termos do artigo 25.º, n.º 6, desta diretiva.
- 56 Além disso, seria contrário ao sistema estabelecido pela Diretiva 95/46, bem como à finalidade dos seus artigos 25.º e 28.º que uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, desta diretiva tivesse como efeito impedir uma autoridade nacional de controlo de apreciar o pedido de uma pessoa relativo aos seus direitos e liberdades no que diz respeito ao tratamento dos seus dados pessoais que tivessem sido ou pudessem ser transferidos de um Estado-Membro para um país terceiro visado por tal decisão.

- 57 Pelo contrário, o artigo 28.º da Diretiva 95/46 aplica-se, pela sua própria natureza, a qualquer tratamento de dados pessoais. Assim, mesmo perante uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, desta diretiva, as autoridades nacionais de controlo às quais uma pessoa tenha apresentado um pedido relativo à proteção dos seus direitos e liberdades no que diz respeito ao tratamento dos seus dados pessoais devem poder examinar, com total independência, se a transferência desses dados respeita as exigências estabelecidas pela referida diretiva.
- 58 Se assim não fosse, as pessoas cujos dados pessoais tivessem sido ou pudessem ser transferidos para o país terceiro em causa ficariam privadas do direito, garantido pelo artigo 8.º, n.ºs 1 e 3, da Carta, de apresentar pedidos às autoridades nacionais de controlo para efeitos da proteção dos seus direitos fundamentais (v., por analogia, acórdão *Digital Rights Ireland e o.*, C-293/12 e C-594/12, EU:C:2014:238, n.º 68).
- 59 Um pedido, nos termos do artigo 28.º, n.º 4, da Diretiva 95/46, através do qual uma pessoa cujos dados pessoais tenham sido ou possam ser transferidos para um país terceiro alega, como no processo principal, que o direito e as práticas desse país não asseguram, não obstante o que a Comissão constatou numa decisão adotada nos termos do artigo 25.º, n.º 6, desta diretiva, um nível de proteção adequado deve ser entendido no sentido de que tem por objeto, em substância, a compatibilidade dessa decisão com a proteção da vida privada e das liberdades e direitos fundamentais das pessoas.
- 60 A este respeito, importa recordar a jurisprudência constante do Tribunal de Justiça segundo a qual a União é uma União de Direito cujas instituições estão sujeitas à fiscalização da conformidade dos seus atos, nomeadamente, com os Tratados, com os princípios gerais do direito e com os direitos fundamentais (v., neste sentido, acórdãos *Comissão e o./Kadi*, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, n.º 66; *Inuit Tapiriit Kanatami e o./Parlamento e Conselho*, C-583/11 P, EU:C:2013:625, n.º 91; e *Telefónica/Comissão*, C-274/12 P, EU:C:2013:852, n.º 56). As decisões da Comissão adotadas nos termos do artigo 25.º, n.º 6, da Diretiva 95/46 não podem, portanto, escapar a tal fiscalização.
- 61 Assim sendo, o Tribunal de Justiça é o único competente para declarar a invalidade de um ato da União, como uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, da Diretiva 95/46, tendo a exclusividade desta competência por objeto garantir a segurança jurídica, preservando a aplicação uniforme do direito da União (v. acórdãos *Melki e Abdeli*, C-188/10 e C-189/10, EU:C:2010:363, n.º 54, e *CIVAD*, C-533/10, EU:C:2012:347, n.º 40).
- 62 Embora possam apreciar a validade de um ato da União, como uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, da Diretiva 95/46, os órgãos jurisdicionais nacionais não têm, todavia, competência para declarar, eles próprios, a invalidade de tal ato (v., neste sentido, acórdãos *Foto-Frost*, 314/85, EU:C:1987:452, n.ºs 15 a 20, e *IATA e ELFAA*, C-344/04, EU:C:2006:10, n.º 27). Por maioria de razão, ao examinarem um pedido, na aceção do artigo 28.º, n.º 4, desta diretiva, relativo à compatibilidade de uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, da referida diretiva com a proteção da vida privada e das liberdades e direitos fundamentais das pessoas, as autoridades nacionais de controlo não têm o direito de declarar, elas próprias, a invalidade de tal decisão.
- 63 Atendendo a estas considerações, quando uma pessoa, cujos dados pessoais tenham sido ou possam ser transferidos para um país terceiro objeto de uma decisão da Comissão nos termos do artigo 25.º, n.º 6, da Diretiva 95/46, apresenta a uma autoridade nacional de controlo um pedido relativo à proteção dos seus direitos e liberdades no que diz respeito ao tratamento desses dados e contesta, por ocasião desse pedido, como acontece no processo principal, a compatibilidade dessa decisão com a proteção da vida privada e das liberdades e direitos fundamentais das pessoas, incumbe a essa autoridade examinar o referido pedido com toda a diligência exigida.

- 64 Na hipótese de a referida autoridade chegar à conclusão de que os elementos apresentados em apoio desse pedido são infundados e, por essa razão, o arquivar, a pessoa que o apresentou deve, como resulta do artigo 28.º, n.º 3, segundo parágrafo, da Diretiva 95/46, lido à luz do artigo 47.º da Carta, ter acesso às vias de recurso jurisdicionais que lhe permitam impugnar essa decisão que lhe é desfavorável perante os órgãos jurisdicionais nacionais. Atendendo à jurisprudência aí referida nos n.ºs 61 e 62 do presente acórdão, esses órgãos jurisdicionais nacionais são obrigados a suspender a instância e a apresentar ao Tribunal de Justiça um pedido de decisão prejudicial de apreciação da validade, quando considerem que um ou vários dos fundamentos de invalidade invocados pelas partes ou, sendo caso disso, suscitados oficiosamente, são procedentes (v., neste sentido, acórdão T & L Sugars e Sidul Açúcares/Comissão, C-456/13 P, EU:C:2015:284, n.º 48 e jurisprudência aí referida).
- 65 Na hipótese contrária, em que considere fundadas as críticas apresentadas pela pessoa que lhe apresentou um pedido relativo à proteção dos seus direitos e liberdades no que diz respeito ao tratamento dos seus dados pessoais, a referida autoridade deve, nos termos do artigo 28.º, n.º 3, primeiro parágrafo, terceiro travessão, da Diretiva 95/46, lido à luz, nomeadamente, do artigo 8.º, n.º 3, da Carta, poder intervir num processo judicial. A este respeito, incumbe ao legislador nacional prever vias de recurso que permitam à autoridade nacional de controlo em causa invocar as críticas que considera fundadas perante os órgãos jurisdicionais nacionais, para que estes últimos, caso partilhem das dúvidas dessa autoridade quanto à validade da decisão da Comissão, procedam a um reenvio prejudicial para efeitos da apreciação da validade dessa decisão.
- 66 Atendendo às considerações anteriores, há que responder às questões submetidas que o artigo 25.º, n.º 6, da Diretiva 95/46, lido à luz dos artigos 7.º, 8.º e 47.º da Carta, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520, através da qual a Comissão constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do artigo 28.º desta diretiva, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado.

Quanto à validade da Decisão 2000/520

- 67 Como resulta das explicações do órgão jurisdicional de reenvio relativas às questões submetidas, M. Schrems alega, no processo principal, que o direito e as práticas dos Estados Unidos não asseguram um nível de proteção adequado na aceção do artigo 25.º da Diretiva 95/46. Como o advogado-geral salientou nos n.ºs 123 e 124 das suas conclusões, M. Schrems expressa dúvidas, que aquele órgão jurisdicional parece, de resto, partilhar em substância, relativas à validade da Decisão 2000/520. Em tais circunstâncias, atendendo às considerações feitas nos n.ºs 60 a 63 do presente acórdão, e a fim de dar uma resposta completa ao referido órgão jurisdicional, importa examinar se essa decisão é conforme às exigências que decorrem da diretiva, lida à luz da Carta.

Quanto às exigências que decorrem do artigo 25.º, n.º 6, da Diretiva 95/46

- 68 Como já foi salientado nos n.ºs 48 e 49 do presente acórdão, o artigo 25.º, n.º 1, da Diretiva 95/46 proíbe as transferências de dados pessoais para países terceiros que não assegurem um nível de proteção adequado.
- 69 Todavia, para efeitos da fiscalização de tais transferências, o artigo 25.º, n.º 6, primeiro parágrafo, desta diretiva dispõe que a Comissão «pode constatar [...] que um país terceiro assegura um nível de proteção adequado na aceção do n.º 2 [desse] artigo em virtude da sua legislação interna ou dos seus compromissos internacionais [...], com vista à proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas».

- 70 É certo que nem o artigo 25.º, n.º 2, nem nenhuma outra disposição da Diretiva 95/46 contêm uma definição do conceito de nível de proteção adequado. Em particular, o artigo 25.º, n.º 2, da referida diretiva limita-se a indicar que a adequação do nível de proteção oferecido por um país terceiro «será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados», e enumera, de modo não exaustivo, as circunstâncias que devem ser tomadas em conta ao proceder a tal apreciação.
- 71 Todavia, por um lado, como resulta dos próprios termos do artigo 25.º, n.º 6, da Diretiva 95/46, esta disposição exige que um país terceiro «assegur[e]» um nível de proteção adequado em virtude da sua legislação interna ou dos seus compromissos internacionais. Por outro lado, também segundo esta disposição, a adequação da proteção assegurada pelo país terceiro é apreciada «com vista à proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas».
- 72 Assim, o artigo 25.º, n.º 6, da Diretiva 95/46 dá execução à obrigação explícita de proteção dos dados pessoais, prevista no artigo 8.º, n.º 1, da Carta, e visa assegurar, como o advogado-geral salientou no n.º 139 das suas conclusões, a continuidade do nível elevado dessa proteção em caso de transferência de dados pessoais para um país terceiro.
- 73 É verdade que o termo «adequado» que figura no artigo 25.º, n.º 6, da Diretiva 95/46 implica que não se pode exigir que um país terceiro assegure um nível de proteção idêntico ao garantido na ordem jurídica da União. Porém, como o advogado-geral salientou no n.º 141 das suas conclusões, a expressão «nível de proteção adequado» deve ser entendida no sentido de que exige que esse país terceiro assegure efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da União nos termos da Diretiva 95/46, lida à luz da Carta. Com efeito, na falta de uma exigência desta natureza, o objetivo referido no número anterior do presente acórdão seria ignorado. Além disso, o elevado nível de proteção garantido pela Diretiva 95/46, lida à luz da Carta, poderia ser facilmente contornado através de transferências de dados pessoais da União para países terceiros com vista ao seu tratamento nesses países.
- 74 Resulta do teor expresso do artigo 25.º, n.º 6, da Diretiva 95/46 que é a ordem jurídica do país terceiro visado pela decisão da Comissão que deve assegurar um nível de proteção adequado. Ainda que, a este respeito, os meios a que esse país recorre para assegurar tal nível de proteção possam ser diferentes dos implementados dentro da União para garantir o cumprimento das exigências que decorrem desta diretiva, lida à luz da Carta, tais meios devem, todavia, revelar-se efetivos, na prática, para assegurar uma proteção substancialmente equivalente à garantida dentro da União.
- 75 Nestas condições, ao examinar o nível de proteção oferecido por um país terceiro, a Comissão está obrigada a apreciar o conteúdo das regras aplicáveis nesse país que resultam da legislação interna ou dos seus compromissos internacionais, bem como a prática destinada a assegurar o respeito de tais regras, devendo, em conformidade com o artigo 25.º, n.º 2, da Diretiva 95/46, tomar em conta todas as circunstâncias relativas a uma transferência de dados pessoais para um país terceiro.
- 76 De igual modo, atendendo ao facto de o nível de proteção assegurado por um país terceiro ser suscetível de evoluir, incumbe à Comissão, após a adoção de uma decisão nos termos do artigo 25.º, n.º 6, da Diretiva 95/46, verificar periodicamente se a constatação relativa ao nível de proteção adequado assegurado pelo país terceiro em causa se continua a justificar de facto e de direito. Tal verificação impõe-se, em qualquer caso, quando haja indícios que suscitem dúvidas a este respeito.
- 77 Além disso, como o advogado-geral salientou nos n.ºs 134 e 135 das suas conclusões, ao examinar a validade de uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, da Diretiva 95/46, devem igualmente ser tomadas em conta as circunstâncias que ocorram posteriormente à adoção dessa decisão.

78 A este respeito, importa referir que, tendo em conta, por um lado, o importante papel desempenhado pela proteção de dados pessoais à luz do direito fundamental ao respeito da vida privada e, por outro, o elevado número de pessoas cujos direitos fundamentais podem ser violados em caso de transferência de dados pessoais para um país terceiro que não assegure um nível de proteção adequado, o poder de apreciação da Comissão quanto à adequação do nível de proteção assegurado por um país terceiro é reduzido, pelo que se deve proceder a uma fiscalização estrita das exigências que decorrem do artigo 25.º da Diretiva 95/46, lido à luz da Carta (v., por analogia, acórdão *Digital Rights Ireland* e o., C-293/12 e C-594/12, EU:C:2014:238, n.ºs 47 e 48).

Quanto ao artigo 1.º da Decisão 2000/520

79 A Comissão considerou, no artigo 1.º, n.º 1, da Decisão 2000/520, que os princípios mencionados no seu anexo I, aplicados em conformidade com as orientações fornecidas pelas FAQ referidas no anexo II da referida decisão, asseguram um nível adequado de proteção dos dados pessoais transferidos a partir da União para organizações estabelecidas nos Estados Unidos. Resulta desta disposição que tanto esses princípios como essas FAQ foram publicados pelo Department of Commerce americano.

80 A adesão de uma organização aos princípios de porto seguro é feita com base num sistema de autocertificação, como resulta do artigo 1.º, n.ºs 2 e 3, dessa decisão, conjugado com a FAQ 6 que figura no anexo II da referida decisão.

81 Embora o recurso, por um país terceiro, a um sistema de autocertificação não seja, em si mesmo, contrário à exigência prevista no artigo 25.º, n.º 6, da Diretiva 95/46, segundo a qual o país terceiro em causa deve assegurar um nível de proteção adequado «em virtude da [...] legislação interna ou dos [...] compromissos internacionais» desse país, a fiabilidade de tal sistema, à luz desta exigência, assenta, essencialmente, na implementação de mecanismos eficazes de deteção e de fiscalização que permitam identificar e punir, na prática, eventuais violações das regras que asseguram a proteção dos direitos fundamentais, nomeadamente o direito ao respeito da vida privada bem como o direito à proteção dos dados pessoais.

82 No caso vertente, por força do anexo I, segundo parágrafo, da Decisão 2000/520, os princípios de porto seguro «[d]estinam-se a ser utilizados exclusivamente por organizações dos EUA que recebam dados pessoais da União Europeia para efeitos de reconhecimento como ‘porto seguro’ e para a presunção de ‘adequação’ implicada nesse processo». Estes princípios são, portanto, unicamente aplicáveis às organizações americanas autocertificadas que recebam dados pessoais da União, sem que se exija que as autoridades públicas americanas fiquem sujeitas ao respeito de tais princípios.

83 Além disso, nos termos do artigo 2.º da Decisão 2000/520, esta «diz respeito tão só ao nível adequado de proteção previsto nos Estados Unidos da América nos termos dos princípios [de porto seguro] aplicados nos termos da[s] FAQ a fim de dar cumprimento ao disposto no n.º 1 do artigo 25.º da Diretiva [95/46]», sem, todavia, conter as constatações suficientes quanto às medidas através das quais os Estados Unidos da América asseguram um nível de proteção adequado, na aceção do artigo 25.º, n.º 6, desta diretiva, em virtude da sua legislação interna ou dos seus compromissos internacionais.

84 Acresce que, em conformidade com o anexo I, quarto parágrafo, da Decisão 2000/520, a aplicabilidade dos referidos princípios pode ser limitada, nomeadamente, por «requisitos de segurança nacional, interesse público ou [cumprimento da lei]», bem como por «legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores [prosseguidos] por essa autorização».

- 85 A este respeito, no título B do seu anexo IV, a Decisão 2000/520 sublinha, no que respeita aos limites a que está sujeita a aplicabilidade dos princípios de porto seguro, que «[c]laramente, sempre que a legislação norte-americana impõe uma obrigação contraditória, as organizações norte-americanas, aderentes ou não ao ‘porto seguro’ têm que aplicar a lei».
- 86 Assim, a Decisão 2000/520 consagra o primado dos «requisitos de segurança nacional, interesse público ou [cumprimento da lei]» sobre os princípios de porto seguro, primado por força do qual as organizações americanas autocertificadas que recebem dados pessoais da União estão obrigadas a afastar, sem limitação, esses princípios quando estes últimos entrem em conflito com aqueles requisitos e se revelem, portanto, incompatíveis com os mesmos.
- 87 Atendendo ao carácter geral da derrogação que figura no anexo I, quarto parágrafo, da Decisão 2000/520, esta possibilita, assim, ingerências, baseadas em requisitos relativos à segurança nacional e ao interesse público ou na legislação interna dos Estados Unidos, nos direitos fundamentais das pessoas cujos dados pessoais sejam ou possam ser transferidos da União para os Estados Unidos. A este respeito, para demonstrar a existência de uma ingerência no direito fundamental ao respeito da vida privada, pouco importa que as informações relativas à vida privada em questão tenham ou não carácter sensível, ou que os interessados tenham ou não sofrido eventuais inconvenientes em razão dessa ingerência (acórdão *Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 33 e jurisprudência aí referida*).
- 88 Além disso, a Decisão 2000/520 não contém qualquer referência à existência, nos Estados Unidos, de normas de carácter estatal destinadas a limitar as eventuais ingerências nos direitos fundamentais das pessoas cujos dados pessoais sejam transferidos da União para os Estados Unidos, ingerências essas que as autoridades estatais deste país seriam autorizadas a praticar quando prosseguem objetivos legítimos, tais como a segurança nacional.
- 89 Acresce que a Decisão 2000/520 não refere a existência de uma proteção jurídica eficaz contra ingerências desta natureza. Como o advogado-geral salientou nos n.ºs 204 a 206 das suas conclusões, os mecanismos de arbitragem privada e os processos perante a Federal Trade Commission (FTC), cujos poderes, descritos, nomeadamente, nas FAQ 11 que figuram no anexo II dessa decisão, estão limitados aos litígios comerciais, têm por objeto o cumprimento, por parte das empresas americanas, dos princípios de porto seguro, e não podem ser aplicados no âmbito de litígios relativos à legalidade de ingerências nos direitos fundamentais que resultem de medidas de origem estatal.
- 90 Por outro lado, a análise da Decisão 2000/520 precedente é corroborada pela apreciação que a própria Comissão fez da situação resultante da aplicação dessa decisão. Com efeito, em particular nos pontos 2 e 3.2 da Comunicação COM(2013) 846 final bem como nos pontos 7.1, 7.2 e 8 da Comunicação COM(2013) 847 final, cujo teor foi exposto, respetivamente, nos n.ºs 13 a 16 bem como nos n.ºs 22, 23 e 25 do presente acórdão, aquela instituição concluiu que as autoridades americanas podiam aceder aos dados pessoais transferidos dos Estados-Membros para os Estados Unidos e tratá-los de um modo incompatível, nomeadamente, com as finalidades da sua transferência, para além do que era estritamente necessário e proporcionado à proteção da segurança nacional. De igual modo, a Comissão concluiu que os interessados não dispunham de vias de direito administrativas ou judiciais que lhes permitissem, nomeadamente, aceder aos dados que lhes dizem respeito e, sendo caso disso, obter a sua retificação ou supressão.
- 91 No que respeita ao nível de proteção das liberdades e direitos fundamentais garantido dentro da União, uma regulamentação dessa proteção que implique uma ingerência nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta deve, segundo a jurisprudência constante do Tribunal de Justiça, estabelecer regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados. A necessidade de dispor destas

garantias é ainda mais importante quando os dados pessoais sejam sujeitos a tratamento automático e exista um risco significativo de acesso ilícito aos mesmos (acórdão *Digital Rights Ireland e o.*, C-293/12 e C-594/12, EU:C:2014:238, n.ºs 54 e 55 bem como jurisprudência aí referida).

- 92 Além disso, e sobretudo, a proteção do direito fundamental ao respeito da vida privada a nível da União exige que as derrogações à proteção dos dados pessoais e as suas limitações operem na estrita medida do necessário (acórdão *Digital Rights Ireland e o.*, C-293/12 e C-594/12, EU:C:2014:238, n.º 52 e jurisprudência aí referida).
- 93 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 [v., neste sentido, no que respeita à 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 L 105, p. 54), acórdão *Digital Rights Ireland e o.*, C-293/12 e C-594/12, EU:C:2014:238, n.ºs 57 a 61].
- 94 Em particular, uma regulamentação que permita às autoridades públicas aceder de modo generalizado ao conteúdo das comunicações eletrónicas deve ser considerada lesiva do conteúdo essencial do direito fundamental ao respeito da vida privada, tal como é garantido pelo artigo 7.º da Carta (v., neste sentido, acórdão *Digital Rights Ireland e o.*, C-293/12 e C-594/12, EU:C:2014:238, n.º 39).
- 95 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, tal como é consagrado no artigo 47.º da Carta. Com efeito, o artigo 47.º, primeiro parágrafo, da Carta exige que qualquer pessoa cujos direitos e liberdades garantidos pelo direito da União tenham sido violados tenha direito a uma ação perante um tribunal nos termos previstos nesse artigo. A este respeito, a própria existência de uma fiscalização jurisdicional efetiva destinada a assegurar o cumprimento das disposições do direito da União é inerente à existência de um Estado de Direito (v., neste sentido, acórdãos *Les Verts/Parlamento*, 294/83, EU:C:1986:166, n.º 23; *Johnston*, 222/84, EU:C:1986:206, n.ºs 18 e 19; *Heylens e o.*, 222/86, EU:C:1987:442, n.º 14; bem como *UGT-Rioja e o.*, C-428/06 a C-434/06, EU:C:2008:488, n.º 80).
- 96 Como se referiu, nomeadamente, nos n.ºs 71, 73 e 74 do presente acórdão, a adoção pela Comissão de uma decisão nos termos do artigo 25.º, n.º 6, da Diretiva 95/46 exige a constatação, devidamente fundamentada, por parte daquela instituição, de que o país terceiro em causa assegura efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção dos direitos fundamentais substancialmente equivalente ao garantido na ordem jurídica da União, como resulta, nomeadamente, dos números anteriores do presente acórdão.
- 97 Ora, há que salientar que a Comissão não indicou, na Decisão 2000/520, que os Estados Unidos da América «asseguram» efetivamente um nível de proteção adequado em virtude da sua legislação interna ou dos seus compromissos internacionais.
- 98 Consequentemente, e sem que seja necessário examinar os princípios de porto seguro quanto ao seu conteúdo, há que concluir que o artigo 1.º daquela decisão viola os requisitos estabelecidos no artigo 25.º, n.º 6, da Diretiva 95/46, lido à luz da Carta, e é, por esta razão, inválido.

Quanto ao artigo 3.º da Decisão 2000/520

- 99 Resulta das considerações expostas nos n.ºs 53, 57 e 63 do presente acórdão que, nos termos do artigo 28.º da Diretiva 95/46, lido à luz, nomeadamente, do artigo 8.º da Carta, as autoridades nacionais de controlo devem poder examinar, com total independência, qualquer pedido relativo à proteção dos direitos e liberdades de uma pessoa no que diz respeito ao tratamento dos seus dados pessoais. Assim é, em particular, quando, por ocasião de tal pedido, essa pessoa suscita interrogações quanto à compatibilidade de uma decisão da Comissão adotada nos termos do artigo 25.º, n.º 6, desta diretiva com a proteção da vida privada e das liberdades e direitos fundamentais das pessoas.
- 100 Todavia, o artigo 3.º, n.º 1, primeiro parágrafo, da Decisão 2000/520 prevê uma regulamentação específica quanto aos poderes de que dispõem as autoridades nacionais de controlo perante uma constatação efetuada pela Comissão relativamente ao nível de proteção adequado, na aceção do artigo 25.º da Diretiva 95/46.
- 101 Assim, nos termos daquela disposição, essas autoridades podem, «[s]em prejuízo da competência para tomar medidas que garantam o cumprimento das disposições nacionais adotadas por força de outras disposições além das previstas no artigo 25.º da Diretiva [95/46], [...] suspender a transferência de dados para uma organização que tenha declarado a sua adesão aos princípios [da Decisão 2000/520]» em condições restritivas que estabeleçam um limiar de intervenção elevado. Embora esta disposição não prejudique os poderes dessas autoridades de tomarem medidas destinadas a assegurar o respeito das disposições nacionais adotadas em execução daquela diretiva, exclui, em contrapartida, a possibilidade de tais autoridades tomarem medidas destinadas a assegurar o respeito do artigo 25.º da mesma diretiva.
- 102 O artigo 3.º, n.º 1, primeiro parágrafo, da Decisão 2000/520 deve, portanto, ser entendido no sentido de que priva as autoridades nacionais de controlo dos poderes que lhes são conferidos pelo artigo 28.º da Diretiva 95/46 no caso de uma pessoa apresentar, por ocasião de um pedido nos termos desta disposição, elementos suscetíveis de colocar em causa a compatibilidade com a proteção da vida privada e das liberdades e direitos fundamentais das pessoas de uma decisão da Comissão que tenha constatado, com base no artigo 25.º, n.º 6, desta diretiva, que um país terceiro assegura um nível de proteção adequado.
- 103 Ora, o poder de execução atribuído pelo legislador da União à Comissão no artigo 25.º, n.º 6, da Diretiva 95/46 não confere a esta instituição competência para limitar os poderes das autoridades nacionais de controlo referidos no número anterior do presente acórdão.
- 104 Nestas condições, há que concluir que, ao adotar o artigo 3.º da Decisão 2000/520, a Comissão ultrapassou a competência que lhe é atribuída pelo artigo 25.º, n.º 6, da Diretiva 95/46, lido à luz da Carta, e que esse artigo é, por essa razão, inválido.
- 105 Uma vez que os artigos 1.º e 3.º da Decisão 2000/520 são indissociáveis dos artigos 2.º e 4.º, bem como dos anexos da mesma, a sua invalidade tem como efeito afetar a validade dessa decisão na sua totalidade.
- 106 Atendendo a todas as considerações precedentes, há que concluir que a Decisão 2000/520 é inválida.

Quanto às despesas

- 107 Revestindo o processo, quanto às partes na causa principal, a natureza de incidente suscitado perante o órgão jurisdicional de reenvio, compete a este decidir quanto às despesas. As despesas efetuadas pelas outras partes para a apresentação de observações ao Tribunal de Justiça não são reembolsáveis.

Pelos fundamentos expostos, o Tribunal de Justiça (Grande chambre) declara:

- 1) **O artigo 25.º, n.º 6, da 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, conforme alterada pelo Regulamento (CE) n.º 1882/2003 do Parlamento Europeu e do Conselho, de 29 de setembro de 2003, lido à luz dos artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46 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, através da qual a Comissão Europeia constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do artigo 28.º desta diretiva, conforme alterada, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado.**
- 2) **A Decisão 2000/520 é inválida.**

Assinatura