Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção)

16 de julho de 2020*

«Reenvio prejudicial — Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.º, 8.º e 47.º — Regulamento (UE) 2016/679 — Artigo 2.º, n.º 2 — Âmbito de aplicação — Transferências de dados pessoais para países terceiros para fins comerciais — Artigo 45.º — Decisão de adequação da Comissão — Artigo 46.º — Transferências mediante garantias adequadas — Artigo 58.º — Poderes das autoridades de controlo — Tratamento dos dados transferidos pelas autoridades públicas de um país terceiro para efeitos de segurança nacional — Apreciação do caráter adequado do nível de proteção assegurado no país terceiro — Decisão 2010/87/UE — Cláusulas-tipo de proteção para a transferência de dados pessoais para países terceiros — Garantias adequadas oferecidas pelo responsável pelo tratamento — Validade — Decisão de Execução (UE) 2016/1250 — Adequação da proteção assegurada pelo Escudo de Proteção da Privacidade União Europeia-Estados Unidos — Validade — Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos»

No processo C-311/18,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pela High Court (Tribunal Superior, Irlanda), por Decisão de 4 de maio de 2018, que deu entrada no Tribunal de Justiça em 9 de maio de 2018, no processo

Data Protection Commissioner

contra

Facebook Ireland Ltd,

Maximillian Schrems,

sendo intervenientes:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

* Língua do processo: inglês.

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: K. Lenaerts, presidente, R. Silva de Lapuerta, vice-presidente, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, L. S. Rossi e I. Jarukaitis, presidentes de secção, M. Ilešič, T. von Danwitz (relator) e D. Šváby, juízes,

advogado-geral: H. Saugmandsgaard Øe,

secretário: C. Strömholm, administradora,

vistos os autos e após a audiência de 9 de julho de 2019,

considerando as observações apresentadas:

– em representação do Data Protection Commissioner, por D. Young, solicitor, B. Murray e M. Collins, SC, e C. Donnelly, BL,

– em representação da Facebook Ireland Ltd, por P. Gallagher e N. Hyland, SC, A. Mulligan e F. Kieran, BL, e P. Nolan, C. Monaghan, C. O'Neill e R. Woulfe, solicitors,

– em representação de M. Schrems, por H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty e S. O'Sullivan, SC, e G. Rudden, solicitor,

– em representação de The United States of America, por E. Barrington, SC, S. Kingston, BL, e S. Barton e B. Walsh, solicitors,

– em representação do Electronic Privacy Information Centre, por S. Lucey, solicitor, G. Gilmore e A. Butler, BL, e C. O'Dwyer, SC,

– em representação da BSA Business Software Alliance Inc., por B. Van Vooren e K. Van Quathem, advocaten,

– em representação da Digitaleurope, por N. Cahill, barrister, J. Cahir, solicitor, e M. Cush, SC,

– em representação da Irlanda, por A. Joyce e M. Browne, na qualidade de agentes, assistidos por D. Fennelly, BL,

– em representação do Governo belga, por J.-C. Halleux e P. Cottin, na qualidade de agentes,

– em representação do Governo checo, por M. Smolek, J. Vláčil, O. Serdula e A. Kasalická, na qualidade de agentes,

– em representação do Governo alemão, por J. Möller, D. Klebs e T. Henze, na qualidade de agentes,

– em representação do Governo francês, por A.-L. Desjonquères, na qualidade de agente,

– em representação do Governo neerlandês, por C. S. Schillemans, M. K. Bulterman e M. Noort, na qualidade de agentes,

– em representação do Governo austríaco, por J. Schmoll e G. Kunnert, na qualidade de agentes,

– em representação do Governo polaco, por B. Majczyna, na qualidade de agente,

– em representação do Governo português, por L. Inez Fernandes, A. Pimenta e C. Vieira Guerra, na qualidade de agentes,

– em representação do Governo do Reino Unido, por S. Brandon, na qualidade de agente, assistido por J. Holmes, QC, e C. Knight, barrister,

– em representação do Parlamento Europeu, por M. J. Martínez Iglesias e A. Caiola, na qualidade de agentes,

– em representação da Comissão Europeia, por D. Nardi, H. Krämer e H. Kranenborg, na qualidade de agentes,

– em representação do Comité Europeu para a Proteção de Dados (EDPB), por A. Jelinek e K. Behn, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 19 de dezembro de 2019,

profere o presente

Acórdão

1 O pedido de decisão prejudicial tem por objeto, em substância,

– a interpretação do artigo 3.º, n.º 2, primeiro travessão, dos artigos 25.º e 26.º, bem como do artigo 28.º, n.º 3, 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 1995, L 281, p. 31), lidos à luz do artigo 4.º, n.º 2, TUE e dos artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»),

– a interpretação e a validade da Decisão 2010/87/UE da Comissão, de 5 de fevereiro de 2010, relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46 (JO 2010, L 39, p. 5), conforme alterada pela Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de dezembro de 2016 (JO 2016, L 344, p. 100) (a seguir «Decisão CPT»), e

– a interpretação e a validade da Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46 (JO 2016, L 207, p. 1; a seguir «Decisão BPD»).

2 Este pedido foi apresentado no âmbito de um litígio que opõe o Data Protection Commissioner (Comissário para a Proteção de Dados, Irlanda) (a seguir «Comissário») à Facebook Ireland Ltd e a Maximillian Schrems a respeito de uma queixa apresentada por este, relativa à transferência dos seus dados pessoais pela Facebook Ireland para a Facebook Inc. nos Estados Unidos.

Quadro jurídico

Diretiva 95/46

3 O artigo 3.º da Diretiva 95/46, sob a epígrafe «Âmbito de aplicação», enunciava, no seu n.º 2:

«A presente diretiva não se aplica ao tratamento de dados pessoais:

– efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado, quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal,

[…]»

4 O artigo 25.º desta diretiva dispunha:

«1. Os Estados-Membros estabelecerão que a transferência para um país terceiro de dados pessoais […] 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; […]

[…]

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.»

5 O artigo 26.º, n.ºs 2 e 4, da referida diretiva previa:

«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.

[…]

4. Sempre que a Comissão decidir, nos termos do procedimento previsto no n.º 2 do artigo 31.º, que certas cláusulas contratuais-tipo oferecem as garantias suficientes referidas no n.º 2, os Estados-Membros tomarão as medidas necessárias para dar cumprimento à decisão da Comissão.»

6 Nos termos do artigo 28.º, n.º 3, da mesma diretiva:

«Cada autoridade d[e] 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 execução 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.

[…]»

RGPD

7 A Diretiva 95/46 foi revogada e substituída pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO 2016, L 119, p. 1; a seguir «RGPD»).

8 Os considerandos 6, 10, 101, 103, 104, 107 a 109, 114, 116 e 141 do RGPD enunciam:

«(6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

[…]

(10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de

manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais ("dados sensíveis"). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.

[…]

(101) A circulação de dados pessoais, com origem e destino quer a países não pertencentes à União quer a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais. O aumento dessa circulação criou novos desafios e novas preocupações em relação à proteção dos dados pessoais. Todavia, quando os dados pessoais são transferidos da União para responsáveis pelo tratamento, para subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional. Em todo o caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento. Só poderão ser realizadas transferências se, sob reserva das demais disposições do presente regulamento, as condições constantes das disposições do presente regulamento relativas a transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante.

[…]

(103) A Comissão pode decidir, com efeitos no conjunto da União, que um país terceiro, um território ou um setor determinado de um país terceiro, ou uma organização internacional, oferece um nível adequado de proteção de dados adequado, garantindo assim a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro ou à organização internacional que seja considerado apto a assegurar tal nível de proteção. Nestes casos, podem realizar-se transferências de dados pessoais para esse país ou organização internacional sem que para tal seja necessária mais nenhuma autorização. A Comissão pode igualmente decidir, após enviar ao país terceiro ou organização internacional uma notificação e uma declaração completa dos motivos, revogar essa decisão.

(104) Em conformidade com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou setor específico de um país terceiro, ter em consideração em que medida esse país respeita o primado do Estado de direito, o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativamente a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União, nomeadamente quando os dados pessoais são tratados num ou mais setores específicos. Em especial, o país terceiro deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer regras de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial.

[…]

(107) A Comissão pode reconhecer que um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, deixou de assegurar um nível adequado de proteção de dados. Por conseguinte, deverá ser proibida a transferência de dados pessoais para esse país terceiro ou organização internacional, a menos que sejam cumpridos os requisitos constantes do presente regulamento relativos a transferências sujeitas a garantias adequadas, incluindo regras vinculativas aplicáveis às empresas, e derrogações para situações específicas. Nesse caso, deverão ser tomadas medidas que visem uma consulta entre a Comissão e esse país terceiro ou organização internacional. A Comissão deverá, em tempo útil, informar o país terceiro ou a organização internacional das razões da proibição e iniciar consultas com o país ou organização em causa, a fim de corrigir a situação.

(108) Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento ou o subcontratante deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade. Essas medidas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indemnização, quer no território da União quer num país terceiro. Deverão estar relacionadas, em especial, com o respeito pelos princípios gerais relativos ao tratamento de dados pessoais e pelos princípios de proteção de dados desde a conceção e por defeito. […]

(109) A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo não os deverá impedir de incluírem estas cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados. Os responsáveis pelo tratamento e os subcontratantes deverão ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção.

[…]

(114) Em qualquer caso, se a Comissão não tiver tomado nenhuma decisão relativamente ao nível de proteção adequado de dados num determinado país terceiro, o responsável pelo tratamento ou o subcontratante deverá adotar soluções que confiram aos titulares dos dados direitos efetivos e oponíveis quanto ao tratamento dos seus dados na União, após a transferência dos mesmos, e lhes garantam que continuarão a beneficiar dos direitos e garantias fundamentais.

[…]

(116) Sempre que dados pessoais atravessarem fronteiras fora do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas

fronteiras. Os seus esforços para colaborar no contexto transfronteiras podem ser também restringidos por poderes preventivos ou medidas de reparação insuficientes, regimes jurídicos incoerentes e obstáculos práticos, tais como a limitação de recursos. […]

[…]

(141) Os titulares dos dados deverão ter direito a apresentar reclamação a uma única autoridade de controlo única, particularmente no Estado-Membro da sua residência habitual, e direito a uma ação judicial efetiva, nos termos do artigo 47.º da Carta, se considerarem que os direitos que lhes são conferidos pelo presente regulamento foram violados ou se a autoridade de controlo não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas necessárias para proteger os seus direitos. […]»

9 O artigo 2.º, n.ºs 1 e 2, deste regulamento prevê:

«1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

2. O presente regulamento não se aplica ao tratamento de dados pessoais:

a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;

b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do [Tratado da União Europeia];

c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;

d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.»

10 O artigo 4.º do referido regulamento dispõe:

«Para efeitos do presente regulamento, entende-se por:

[…]

2) "Tratamento", uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

[…]

7) "Responsável do tratamento", a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;

8) "Subcontratante", uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

9) "Destinatário", uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento;

[…]»

11 O artigo 23.º do mesmo regulamento enuncia:

«1. O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:

a) A segurança do Estado;

b) A defesa;

c) A segurança pública;

d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;

[…]

2. Em especial, as medidas legislativas referidas no n.º 1 incluem, quando for relevante, disposições explícitas relativas, pelo menos:

a) Às finalidades do tratamento ou às diferentes categorias de tratamento;

b) Às categorias de dados pessoais;

c) Ao alcance das limitações impostas;

d) Às garantias para evitar o abuso ou o acesso ou transferência ilícitos;

e) À especificação do responsável pelo tratamento ou às categorias de responsáveis pelo tratamento;

f) Aos prazos de conservação e às garantias aplicáveis, tendo em conta a natureza, o âmbito e os objetivos do tratamento ou das categorias de tratamento;

g) Aos riscos específicos para os direitos e liberdades dos titulares dos dados; e

h) Ao direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.»

12 O capítulo V do RGPD, sob a epígrafe «Transferências de dados pessoais para países terceiros ou organizações internacionais», inclui os artigos 44.º a 50.º deste regulamento. Nos termos do seu artigo 44.º, sob a epígrafe «Princípio geral das transferências»:

«Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento.»

13 O artigo 45.º deste regulamento, sob a epígrafe «Transferências com base numa decisão de adequação», prevê, nos seus n.os 1 a 3:

«1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.

2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:

a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;

b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e

c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

3. Após avaliar a adequação do nível de proteção, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado na aceção do n.º 2 do presente artigo. O ato de execução prevê um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional. O ato de execução especifica o âmbito de aplicação territorial e setorial e, se for caso disso, identifica a autoridade ou autoridades de controlo a que se refere o n.º 2, alínea b), do presente artigo. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.»

14 O artigo 46.º do referido regulamento, sob a epígrafe «Transferências sujeitas a garantias adequadas», dispõe, nos seus n.os 1 a 3:

«1. Não tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

2. Podem ser previstas as garantias adequadas referidas no n.º 1, sem requerer nenhuma autorização específica de uma autoridade de controlo, por meio de:

a) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;

b) Regras vinculativas aplicáveis às empresas em conformidade com o artigo 47.º;

c) Cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2;

d) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2;

e) Um código de conduta, aprovado nos termos do artigo 40.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou

f) Um procedimento de certificação, aprovado nos termos do artigo 42.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados.

3. Sob reserva de autorização da autoridade de controlo competente, podem também ser previstas as garantias adequadas referidas no n.º 1, nomeadamente por meio de:

a) Cláusulas contratuais entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou organização internacional; ou

b) Disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.»

15 O artigo 49.º do mesmo regulamento, sob a epígrafe «Derrogações para situações específicas», enuncia:

«1. Na falta de uma decisão de adequação nos termos do artigo 45.º, n.º 3, ou de garantias adequadas nos termos do artigo 46.º, designadamente de regras vinculativas aplicáveis às empresas, as transferências ou conjunto de transferências de dados pessoais para países terceiros ou organizações internacionais só são efetuadas caso se verifique uma das seguintes condições:

a) O titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;

b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;

c) A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou coletiva;

d) A transferência for necessária por importantes razões de interesse público;

e) A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;

f) A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento;

g) A transferência for realizada a partir de um registo que, nos termos do direito da União ou do Estado-Membro, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito da União ou de um Estado-Membro se encontrem preenchidas nesse caso concreto.

Quando uma transferência não puder basear-se no disposto no artigo 45.º ou 46.º, incluindo nas regras vinculativas aplicáveis às empresas, e não for aplicável nenhuma das derrogações previstas para as situações específicas a que se refere o primeiro parágrafo do presente número, a transferência para um país terceiro ou uma organização internacional só pode ser efetuada se não for repetitiva, apenas disser respeito a um número limitado de titulares dos dados, for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados, e o responsável pelo tratamento tiver ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tiver apresentado garantias adequadas no que respeita à proteção de dados pessoais. O responsável pelo tratamento informa da transferência a autoridade de controlo. Para além de fornecer a informação referida nos artigos 13.º e 14.º, o responsável pelo tratamento presta informações ao titular dos dados sobre a transferência e os interesses legítimos visados.

2. As transferências efetuadas nos termos do n.º 1, primeiro parágrafo, alínea g), não envolvem a totalidade dos dados pessoais nem categorias completas de dados pessoais constantes do registo. Quando o registo se destinar a ser consultado por pessoas com um interesse legítimo, as transferências só podem ser efetuadas a pedido dessas pessoas ou se forem elas os seus destinatários.

3. O n.º 1, primeiro parágrafo, alíneas a), b) e c), e segundo parágrafo, não é aplicável a atividades levadas a cabo por autoridades públicas no exercício dos seus poderes.

4. O interesse público referido no n.º 1, primeiro parágrafo, alínea d), é reconhecido pelo direito da União ou pelo direito do Estado-Membro a que o responsável pelo tratamento se encontre sujeito.

5. Na falta de uma decisão de adequação, o direito da União ou de um Estado-Membro podem, por razões importantes de interesse público, estabelecer expressamente limites à transferência de categorias específicas de dados para países terceiros ou organizações internacionais. Os Estados-Membros notificam a Comissão dessas disposições.

6. O responsável pelo tratamento ou o subcontratante documenta a avaliação, bem como as garantias adequadas referidas no n.º 1, segundo parágrafo, do presente artigo, nos registos a que se refere o artigo 30.º»

16 Nos termos do artigo 51.º, n.º 1, do RGPD:

«Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União ("autoridade de controlo").»

17 Em conformidade com o artigo 55.º, n.º 1, deste regulamento, «[a]s autoridades de controlo são competentes para prosseguir as atribuições e exercer os poderes que lhes são conferidos pelo presente regulamento no território do seu próprio Estado-Membro».

18 O artigo 57.º, n.º 1, do referido regulamento prevê:

«Sem prejuízo de outras atribuições previstas nos termos do presente regulamento, cada autoridade de controlo, no território respetivo:

a) Controla e executa a aplicação do presente regulamento;

[…]

f) Trata as reclamações apresentadas por qualquer titular de dados […] e investigar, na medida do necessário, o conteúdo da reclamação e informar o autor da reclamação do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo;

[…]»

19 Nos termos do artigo 58.º, n.ºs 2 e 4, do mesmo regulamento:

«2. Cada autoridade de controlo dispõe dos seguintes poderes de correção:

[…]

f) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição;

[…]

j) Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais.

[…]

4. O exercício dos poderes conferidos à autoridade de controlo nos termos do presente artigo está sujeito a garantias adequadas, que incluem o direito à ação judicial efetiva e a um processo equitativo, previstas no direito da União e dos Estados-Membros, em conformidade com a Carta.»

20 O artigo 64.º, n.º 2, do RGPD enuncia:

«As autoridades de controlo, o presidente do [Comité Europeu para a Proteção de Dados (EDPB)] ou a Comissão podem solicitar que o Comité analise qualquer assunto de aplicação geral ou que produza efeitos em mais do que um Estado-Membro, com vista a obter um parecer, nomeadamente se a autoridade de controlo competente não cumprir as obrigações em matéria de assistência mútua previstas no artigo 61.º ou de operações conjuntas previstas no artigo 62.º»

21 Nos termos do artigo 65.º, n.º 1, deste regulamento:

«A fim de assegurar a aplicação correta e coerente do presente regulamento em cada caso, o Comité adota uma decisão vinculativa nos seguintes casos:

[…]

c) Quando a autoridade de controlo competente não solicitar o parecer do Comité nos casos referidos no artigo 64.º, n.º 1, ou não seguir o parecer do Comité emitido nos termos do artigo 64.º Nesse caso, qualquer autoridade de controlo interessada, ou a Comissão, pode remeter o assunto para o Comité.»

22 O artigo 77.º do referido regulamento, sob a epígrafe «Direito de apresentar reclamação a uma autoridade de controlo», enuncia:

«1. Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm direito a apresentar reclamação a uma autoridade de controlo, em especial no Estado-Membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada a infração, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diga respeito viola o presente regulamento.

2. A autoridade de controlo à qual tiver sido apresentada a reclamação informa o autor da reclamação sobre o andamento e o resultado da reclamação, inclusive sobre a possibilidade de intentar ação judicial nos termos do artigo 78.º»

23 O artigo 78.º do mesmo regulamento, sob a epígrafe «Direito à ação judicial contra uma autoridade de controlo», prevê, nos seus n.os 1 e 2:

«1. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, todas as pessoas singulares ou coletivas têm direito à ação judicial contra as decisões juridicamente vinculativas das autoridades de controlo que lhes digam respeito.

2. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, os titulares dos dados têm direito à ação judicial se a autoridade de controlo competente nos termos dos artigos 55.º e 56.º não tratar a reclamação ou não informar o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da reclamação que tenha apresentado nos termos do artigo 77.º»

24 O artigo 94.º do RGPD dispõe:

«1. A Diretiva [95/46] é revogada com efeitos a partir de 25 de maio de 2018.

2. As remissões para a diretiva revogada são consideradas remissões para presente regulamento. As referências ao Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, criado pelo artigo 29.º da Diretiva [95/46], são consideradas referências ao Comité Europeu para a Proteção de Dados criado pelo presente regulamento.»

25 Nos termos do artigo 99.º deste regulamento:

«1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

2. O presente regulamento é aplicável a partir de 25 de maio de 2018.»

Decisão CPT

26 O considerando 11 da Decisão CPT tem a seguinte redação:

«As autoridades de controlo dos Estados-Membros desempenham um papel fundamental neste mecanismo contratual, assegurando uma proteção adequada dos dados após a sua transferência. Nos casos excecionais em que os exportadores de dados se recusem ou não estejam em condições de fornecer instruções adequadas aos importadores de dados, podendo, dessa forma, prejudicar gravemente os titulares dos dados, as cláusulas contratuais-tipo devem permitir às autoridades de controlo realizar auditorias junto dos importadores de dados e dos seus subcontratantes e, se for caso disso, tomar decisões que vinculem esses importadores de dados e os seus subcontratantes. As autoridades de controlo dos Estados-Membros devem poder proibir ou suspender uma transferência ou um conjunto de transferências de dados com base nas cláusulas contratuais-tipo, nos casos excecionais em que se verifique que uma transferência efetuada numa base contratual é suscetível de ter um efeito adverso importante nas garantias e obrigações que oferecem uma proteção adequada ao titular dos dados.»

27 O artigo 1.º desta decisão dispõe:

«Considera-se que as cláusulas contratuais-tipo constantes do anexo oferecem garantias adequadas de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respetivos direitos, tal como exigido no artigo 26.º, n.º 2, da Diretiva [95/46].»

28 Em conformidade com o artigo 2.º, segundo parágrafo, da referida decisão, esta «aplica-se à transferência de dados pessoais efetuada por responsáveis pelo tratamento estabelecidos na União Europeia para destinatários estabelecidos fora do território da União Europeia que atuem apenas como subcontratantes».

29 O artigo 3.º da mesma decisão dispõe:

«Para efeitos do disposto na presente decisão, entende-se por:

[…]

c) "Exportador de dados", o responsável pelo tratamento que transfere dados pessoais;

d) "Importador de dados", o subcontratante estabelecido num país terceiro que concorda em receber, do exportador de dados, dados pessoais para serem tratados por conta deste depois da transferência, em conformidade com as suas instruções e nos termos da presente decisão, e que não está sujeito a um sistema de um país terceiro que assegure uma proteção adequada, na aceção do artigo 25.º, n.º 1, da Diretiva [95/46];

[…]

f) "Legislação sobre proteção de dados aplicável", a legislação que protege os direitos e as liberdades fundamentais das pessoas e, em especial, o seu direito à proteção da vida privada no que diz respeito ao tratamento dos seus dados pessoais, aplicável a um responsável pelo tratamento dos dados no Estado-Membro em que o exportador de dados está estabelecido;

[…]»

30 Na sua versão inicial, anterior à entrada em vigor da Decisão de Execução 2016/2297, o artigo 4.º da Decisão 2010/87 previa:

«1. Sem prejuízo das suas competências para tomar medidas que garantam o cumprimento das disposições nacionais adotadas por força dos capítulos II, III, V e VI da Diretiva [95/46], as autoridades competentes dos Estados-Membros podem exercer as suas competências para proibir ou suspender o fluxo de dados para países terceiros, de forma a proteger as pessoas no que diz respeito ao tratamento dos seus dados pessoais, nos casos em que:

a) Esteja comprovado que a legislação a que o importador de dados ou um subcontratante ulterior está sujeito lhe impõe requisitos que lhe permitem derrogar à legislação sobre proteção de dados aplicável e que ultrapassam as restrições necessárias numa sociedade democrática, tal como previsto no artigo 13.º da Diretiva [95/46], sempre que estes requisitos possam ter um efeito adverso substancial nas garantias fornecidas pela legislação sobre proteção de dados aplicável e pelas cláusulas contratuais-tipo;

b) Seja determinado, por uma entidade competente, que o importador de dados ou um subcontratante ulterior não respeitou as cláusulas contratuais-tipo constantes do anexo; ou

c) Existam fortes probabilidades de as cláusulas contratuais-tipo constantes do anexo não estarem a ser ou não virem a ser cumpridas e de a continuação da transferência dos dados poder causar graves prejuízos aos titulares dos dados.

2. A proibição ou suspensão prevista no n.º 1 é levantada assim que as razões que estiveram na sua origem deixarem de existir.

3. Quando os Estados-Membros adotarem medidas em conformidade com os n.os 1 e 2, informarão o mais rapidamente possível a Comissão, a qual, por sua vez, informará os outros Estados-Membros.»

31 O considerando 5 da Decisão de Execução 2016/2297, adotada na sequência da prolação do Acórdão de 6 de outubro de 2015, Schrems (C-362/14, EU:C:2015:650), tem a seguinte redação:

«*Mutatis mutandis*, uma decisão adotada pela Comissão nos termos do artigo 26.º, n.º 4, da Diretiva [95/46] é vinculativa para todos os organismos dos Estados-Membros aos quais se destina, nomeadamente para as suas autoridades independentes de supervisão, na medida em que tem por efeito o reconhecimento de que as transferências efetuadas com base em cláusulas contratuais-tipo nela estabelecidas oferecem as garantias suficientes referidas no artigo 26.º, n.º 2, da referida diretiva. Tal não impede uma autoridade nacional de controlo de exercer as suas competências de supervisão dos fluxos de dados, incluindo o poder de suspender ou de proibir uma transferência de dados pessoais, se considerar que a transferência é efetuada em violação da legislação nacional ou da [União Europeia] em matéria de proteção de dados, nomeadamente quando o importador dos dados não respeite as cláusulas contratuais-tipo.»

32 Na sua versão atual, resultante da Decisão de Execução 2016/2297, o artigo 4.º da Decisão CPT enuncia:

«Sempre que as autoridades competentes dos Estados-Membros exerçam os seus poderes nos termos do artigo 28.º, n.º 3, da Diretiva [95/46], conduzindo assim à suspensão ou proibição definitiva dos fluxos de dados para países terceiros a fim de proteger pessoas singulares no que respeita ao tratamento dos seus dados pessoais, o Estado-Membro em causa deve, sem demora, informar a Comissão, a qual, por sua vez, informará os outros Estados-Membros.»

33 O anexo da Decisão CPT, sob a epígrafe «Cláusulas contratuais-tipo (subcontratantes)», inclui doze cláusulas-tipo. A cláusula 3 deste anexo, intitulada «Cláusula do terceiro beneficiário», prevê:

«1. O titular dos dados pode fazer aplicar contra o exportador de dados a presente cláusula, a cláusula 4, alíneas b) a i), a cláusula 5, alíneas a) a e) e g) a j), a cláusula 6, n.os 1 e 2, a cláusula 7, a cláusula 8, n.º 2, e as cláusulas 9 a 12, na qualidade de terceiro beneficiário.

2. O titular dos dados pode fazer aplicar, contra o importador de dados a presente cláusula, a cláusula 5, alíneas a) a e) e g), as cláusulas 6 e 7, a cláusula 8, n.º 2, e as cláusulas 9 a 12, em caso de desaparecimento de facto ou de extinção legal do exportador de dados, a menos que qualquer entidade sucessora tenha assumido a totalidade das obrigações legais do exportador de dados mediante contrato ou por força da lei, e consequentemente assuma os direitos e obrigações do exportador de dados, podendo nesse caso o titular dos dados invocá-los contra tal entidade.

[…]»

34 Nos termos da cláusula 4 desse anexo, sob a epígrafe «Obrigações do exportador de dados»:

«O exportador de dados acorda e garante:

a) Que o tratamento dos dados pessoais, incluindo a própria transferência, foi e continuará a ser feito de acordo com as disposições pertinentes da legislação sobre proteção de dados aplicável (e que, se aplicável, foi notificada às entidades competentes do Estado-Membro em que o exportador de dados está estabelecido) e que não viola as disposições pertinentes desse Estado;

b) Que deu e continuará a dar instruções ao importador de dados durante os serviços de tratamento de dados pessoais para tratar os dados pessoais transferidos apenas por conta do exportador de dados e em conformidade com a legislação sobre proteção de dados aplicável e com as cláusulas;

[…]

f) Que, se a transferência envolver categorias especiais de dados, o titular dos dados foi informado ou será informado antes ou o mais depressa possível após a transferência, de que os seus dados poderão ser transmitidos para um país terceiro que não garante um nível de proteção adequado na aceção da Diretiva [95/46];

g) Que enviará qualquer notificação recebida do importador de dados ou de qualquer subcontratante ulterior à autoridade de controlo responsável pela proteção dos dados, nos termos da cláusula 5, alínea b), e da cláusula 8, n.º 3, se decidir continuar a transferência ou levantar a suspensão;

[…]»

35 A cláusula 5 do referido anexo, sob a epígrafe «Obrigações do importador de dados […]», estipula:

«O importador de dados acorda e garante:

a) Que tratará os dados pessoais apenas por conta do exportador de dados e em conformidade com as suas instruções e as cláusulas; no caso de não poder cumprir estas obrigações por qualquer razão, concorda em informar imediatamente o exportador de dados desse facto, tendo neste caso o exportador de dados o direito de suspender a transferência de dados e/ou de rescindir o contrato;

b) Que não tem qualquer razão para crer que a legislação que lhe é aplicável o impede de respeitar as instruções recebidas do exportador de dados e as obrigações que lhe incumbem por força do contrato e que, no caso de haver uma alteração nesta legislação que possa ter um efeito adverso

substancial nas garantias e obrigações conferidas pelas cláusulas, notificará imediatamente essa alteração ao exportador de dados, logo que dela tiver conhecimento, tendo neste caso o exportador de dados o direito de suspender a transferência de dados e/ou de rescindir o contrato;

[…]

d) Que notificará imediatamente o exportador de dados no que respeita a:
   i) qualquer pedido juridicamente vinculativo de divulgação dos dados pessoais por parte de uma autoridade competente para a aplicação da lei, a não ser que exista uma proibição em contrário, como uma proibição prevista no direito penal para preservar a confidencialidade de uma investigação policial;
   ii) qualquer acesso acidental ou não autorizado; e
   iii) qualquer pedido recebido diretamente dos titulares de dados, sem responder a esse pedido, a não ser que tenha sido autorizado a fazê-lo;

[…]»

36 A nota de rodapé para a qual remete a epígrafe desta cláusula 5 enuncia:

«Os requisitos obrigatórios da legislação nacional aplicáveis ao importador de dados que não excedam o necessário numa sociedade democrática, com base num dos interesses enunciados no artigo 13.º, n.º 1, da Diretiva [95/46], ou seja, se constituírem uma medida necessária à proteção da segurança e da defesa do Estado, da segurança pública, da prevenção, investigação, deteção e repressão de infrações penais, ou de violações da deontologia das profissões regulamentadas, de um importante interesse económico ou financeiro do Estado, ou da proteção do titular dos dados ou dos direitos e liberdades de outrem, não são contrários ao disposto nas cláusulas contratuais-tipo. […]»

37 A cláusula 6 do anexo da Decisão CPT, sob a epígrafe «Responsabilidade», prevê:

«1. As partes acordam que qualquer titular dos dados que tenha sofrido danos resultantes de qualquer incumprimento das obrigações referidas nas cláusulas 3 ou 11 por qualquer parte ou subcontratante ulterior tem o direito de obter reparação do exportador de dados pelos danos sofridos.

2. Se o titular dos dados não puder intentar uma ação de reparação em conformidade com o n.º 1 contra o exportador de dados, por incumprimento pelo importador de dados ou o seu subcontratante de quaisquer das suas obrigações referidas nas cláusulas 3 e 11, devido ao desaparecimento de facto ou extinção legal ou à insolvência do exportador de dados, o importador de dados aceita que o titular dos dados lhe possa intentar uma ação como se fosse o exportador de dados […]

[…]»

38 A cláusula 8 deste anexo, sob a epígrafe «Cooperação com as autoridades de controlo», estipula, no seu n.º 2:

«As partes acordam que a autoridade de controlo tem o direito de realizar auditorias ao importador de dados ou a qualquer subcontratante ulterior com o mesmo âmbito e nas mesmas condições das auditorias efetuadas ao exportador de dados, em conformidade com a legislação sobre proteção de dados aplicável.»

39 A cláusula 9 do referido anexo, sob a epígrafe «Direito aplicável», precisa que as cláusulas são regidas pelo direito do Estado-Membro onde o exportador de dados está estabelecido.

40 Nos termos da cláusula 11 do mesmo anexo, sob a epígrafe «Subcontratação ulterior»:

«1. O importador de dados não subcontrata nenhuma das suas atividades de tratamento executadas por conta do exportador de dados ao abrigo das cláusulas sem o consentimento escrito prévio deste. Sempre que o importador de dados subcontratar as suas obrigações ao abrigo das presentes cláusulas, com o consentimento do exportador de dados, fá-lo apenas mediante acordo escrito com o subcontratante ulterior que imponha a este último as mesmas obrigações do importador de dados ao abrigo das cláusulas […].

2. O contrato escrito prévio entre o importador de dados e o subcontratante ulterior deve prever igualmente uma cláusula do terceiro beneficiário, tal como previsto na cláusula 3, para os casos em que o titular dos dados não puder intentar a ação de reparação referida na cláusula 6, n.º 1, contra o exportador ou o importador de dados por estes terem desaparecido de facto ou terem sido extintos legalmente ou por se terem tornado insolventes e nenhuma entidade sucessora ter assumido a totalidade das obrigações do exportador ou do importador de dados, mediante contrato ou por força da lei. Esta responsabilidade civil do subcontratante ulterior é limitada às suas próprias atividades de tratamento de dados ao abrigo das presentes cláusulas.

[…]»

41 A cláusula 12 do anexo da Decisão CPT, sob a epígrafe «Obrigação depois de terminados os serviços de tratamento de dados pessoais», enuncia, no seu n.º 1:

«As partes acordam que, após terminada a prestação de serviços de tratamento de dados, o importador de dados e o seu subcontratante, conforme preferência do exportador de dados, devolverão todos os dados pessoais transferidos e as suas cópias ao exportador de dados ou destruirão todos os dados pessoais e certificarão ao exportador de dados que o fizeram, exceto se a legislação imposta ao importador de dados o impedir de devolver ou destruir a totalidade ou parte dos dados pessoais transferidos. […]»

Decisão BPD

42 Por Acórdão de 6 de outubro de 2015, Schrems (C-362/14, EU:C:2015:650), o Tribunal de Justiça declarou inválida 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 (JO 2000, L 215, p. 7), na qual a Comissão tinha constatado que esse país terceiro assegurava um nível adequado de proteção.

43 Na sequência da prolação desse acórdão, a Comissão adotou a Decisão BPD, após ter procedido, para efeitos da sua adoção, a uma avaliação da regulamentação dos Estados Unidos, como precisa o considerando 65 da referida decisão:

«A Comissão avaliou as limitações e garantias disponíveis na legislação dos EUA no que se refere ao acesso e à utilização de dados pessoais, transferidos ao abrigo do Escudo de Proteção da Privacidade [União Europeia]-EUA, pelas autoridades públicas dos EUA para efeitos de segurança nacional, de exercício de funções coercivas e outros fins de interesse público. Além disso, o Governo dos EUA, através do seu Office of the Director of National Intelligence ODNI) […], apresentou à Comissão declarações e compromissos pormenorizados que constam do anexo VI da presente decisão. Por carta assinada pelo Secretary of State e que figura no anexo III da presente decisão, o Governo dos EUA também se comprometeu a criar um novo mecanismo de supervisão da ingerência da segurança nacional, o Mediador para o Escudo de Proteção da Privacidade, que é independente do setor das informações. Por último, uma declaração do Department of Justice (equivalente ao Ministério da

Justiça) dos EUA, constante do anexo VII da presente decisão, descreve as limitações e garantias aplicáveis ao acesso e à utilização de dados pelas autoridades públicas para efeitos de aplicação da lei e outros fins de interesse público. Para aumentar a transparência e refletir a natureza jurídica destes compromissos, cada um dos documentos enumerados e que figuram em anexo à presente decisão será publicado no Registo Federal dos EUA.»

44 A análise efetuada pela Comissão a essas limitações e garantias está resumida nos considerandos 67 a 135 da Decisão BPD, ao passo que as conclusões desta instituição relativas ao nível adequado de proteção no âmbito do Escudo de Proteção da Privacidade União Europeia-Estados Unidos figuram nos seus considerandos 136 a 141.

45 Em particular, os considerandos 68, 69, 76, 77, 109, 112 a 116, 120, 136 e 140 desta decisão enunciam:

«(68) Nos termos da Constituição dos EUA, o [p]residente, na qualidade de comandante supremo e chefe do Executivo, é responsável por garantir a segurança nacional e, no que diz respeito às informações externas, é responsável pelos negócios estrangeiros dos EUA […]. Embora o Congresso tenha competência para impor limitações, e o tenha feito em vários aspetos, o [p]residente dentro destes limites pode administrar as atividades do setor das informações dos EUA, nomeadamente através de decretos executivos ou diretivas presidenciais. […] Atualmente, os dois instrumentos jurídicos centrais a este respeito são o Decreto Executivo n.º 12333 ("E.O. 12333") […] e a Presidential Policy Directive 28.

(69) A Presidential Policy Directive 28 ("PPD-28"), emitida em 17 de janeiro de 2014, impõe várias limitações às operações de "informação de origem eletromagnética" […]. Esta PPD é vinculativa para os serviços de informações norte-americanos e […] permanece em vigor após a alteração da administração dos EUA […]. A PPD-28 é de especial importância para os cidadãos de países terceiros, nomeadamente para os titulares de dados da [União]. […]

[…]

(76) Embora não enunciados nesses termos jurídicos, estes princípios [da PPD-28] refletem a essência dos princípios d[a] necessidade e [da] proporcionalidade. […]

(77) Enquanto diretiva emitida pelo [p]residente na qualidade de chefe do Executivo, estes requisitos são vinculativos para todo o setor das informações e foram posteriormente aplicados através das normas e procedimentos dos serviços que transpõem os princípios gerais em orientações específicas para as operações quotidianas. […]

[…]

(109) Pelo contrário, nos termos da secção 702 da [Foreign Intelligence Surveillance Act (FISA)] [o United States Foreign Intelligence Surveillance Court (FISC) (Tribunal de Supervisão dos Serviços de Informações Externas dos Estados Unidos)] não autoriza medidas de vigilância individuais; em vez disso, autoriza programas de vigilância (tais como o PRISM e o UPSTREAM) com base em certificações anuais elaboradas pelo [United States Attorney General (procurador-geral)] e o Director of National Intelligence [(DNI) (diretor dos Serviços Nacionais de Informações)]. […] Tal como indicado, as certificações a aprovar pelo FISC não contêm informações sobre as pessoas visadas, mas sim categorias de identificação das informações no estrangeiro […]. Embora o FISC não avalie — com base numa causa provável ou em qualquer outra norma — se as pessoas são adequadamente visadas para efeitos de obtenção de informações externas […], o seu controlo alarga-se à condição de que "um objetivo significativo da recolha consiste na obtenção de informações no estrangeiro" […].

[…]

(112) Em primeiro lugar, a [FISA] prevê várias vias de recurso acessíveis igualmente a cidadãos de países terceiros, a fim de contestar a vigilância eletrónica ilegal […]. O que precede inclui a possibilidade de as pessoas instaurarem uma ação civil de indemnização contra os Estados Unidos sempre que as informações sobre si tenham sido ilegal e intencionalmente utilizadas ou divulgadas […]; instaurarem uma ação de indemnização contra funcionários do Governo dos EUA na sua capacidade pessoal ("no aparente cumprimento da lei") […]; e contestarem a legalidade da vigilância (e solicitarem a supressão das informações) caso o Governo dos EUA tencione utilizar ou divulgar quaisquer informações obtidas ou decorrentes de vigilância eletrónica contra a pessoa em processos judiciais ou administrativos nos Estados Unidos […]

(113) Em segundo lugar, o Governo dos EUA remeteu a Comissão para várias vias de recurso adicionais que os titulares de dados da [União] podem utilizar para efeitos de recurso contra funcionários do governo em virtude do acesso, ou da utilização, ilegal por parte do governo, de dados pessoais, nomeadamente para alegados efeitos de segurança nacional […]

(114) Por último, o Governo dos EUA salientou a [Freedom of Information Act (FOIA) (Lei Relativa à Liberdade de Informação)] como um meio para os cidadãos de países terceiros solicitarem o acesso a documentação existente dos serviços federais, nomeadamente nos casos em que esta contenha os dados pessoais do respetivo titular […]. Devido à sua incidência, a FOIA não prevê uma via de recurso individual contra a ingerência nos dados pessoais como tal, embora possa, em princípio, permitir que as pessoas obtenham acesso a informações relevantes conservadas por serviços de informações nacionais. […]

(115) Embora as pessoas, incluindo os titulares de dados da [União], disponham de várias vias de recurso se tiverem sido objeto de vigilância (eletrónica) ilegal para efeitos de segurança nacional, é igualmente evidente que pelo menos algumas bases jurídicas que os serviços de informações dos EUA podem utilizar (por exemplo E.O. 12333) não são abrangidas. Além disso, mesmo nos casos em que, em princípio, existem possibilidades de recurso judicial para cidadãos de países terceiros, como no que diz respeito à vigilância ao abrigo da FISA, as causas de ação disponíveis são limitadas […] e as ações apresentadas por pessoas singulares (incluindo cidadãos dos EUA) serão declaradas inadmissíveis se não conseguirem demonstrar "legitimidade" […], o que limita o acesso aos tribunais comuns […]

(116) A fim de proporcionar uma via de recurso adicional acessível a todos os titulares de dados da [União], o Governo dos EUA decidiu criar um novo mecanismo de mediação, tal como estabelecido na carta do U.S. Secretary of State à Comissão, que consta do anexo III da presente decisão. Este mecanismo baseia-se na nomeação, nos termos da PPD-28, de um coordenador superior (ao nível de Under-Secretary) no State Department como ponto de contacto junto do qual os governos estrangeiros podem expressar preocupações sobre as atividades de informação de origem eletromagnética dos EUA, mas vai significativamente além deste conceito inicial.

[…]

(120) [O] [G]overno americano compromete-se a garantir que, no exercício das suas funções, o Mediador para o Escudo de Proteção da Privacidade poderá apoiar-se na cooperação de outros mecanismos de verificação do cumprimento e de supervisão previstos no direito dos EUA. […] Nos casos em que um destes organismos de supervisão tenha detetado qualquer incumprimento, os serviços de informação em questão (por exemplo, uma agência de informações) terá de corrigir o incumprimento, uma vez que apenas deste modo o Mediador poderá garantir uma resposta "positiva" à pessoa (ou seja, que se corrigiu o incumprimento), em relação ao qual o [G]overno americano se comprometeu. […]

[…]

(136) Com base nestas conclusões, a Comissão considera que os EUA asseguram um nível de proteção adequado dos dados pessoais transferidos da União para organizações autocertificadas dos Estados Unidos ao abrigo do Escudo de Proteção da Privacidade [União Europeia]-EUA.

[…]

(140) Por último, com base nas informações disponíveis sobre a ordem jurídica dos EUA, designadamente as declarações e compromissos do [G]overno dos EUA, a Comissão considera que qualquer ingerência por parte das autoridades públicas dos EUA nos direitos fundamentais das pessoas cujos dados são transferidos da União para os Estados Unidos da América ao abrigo do Escudo de Proteção da Privacidade para efeitos de segurança nacional, do exercício de funções coercivas ou outros efeitos de interesse público, e as subsequentes restrições impostas às organizações autocertificadas no que se refere à sua adesão aos princípios, serão limitadas ao que é estritamente necessário para a consecução do objetivo legítimo em questão, e que existe uma proteção jurídica eficaz contra tal ingerência.»

46 Nos termos do artigo 1.º da Decisão BPD:

«1. Para efeitos do artigo 25.º, n.º 2, da Diretiva [95/46], os Estados Unidos devem assegurar um nível de proteção adequado dos dados pessoais transferidos da União para organizações dos Estados Unidos ao abrigo do Escudo de Proteção da Privacidade [União Europeia]-EUA.

2. O Escudo de Proteção da Privacidade [União Europeia]-EUA é constituído pelos princípios emitidos pelo Department of Commerce dos EUA em 7 de julho de 2016, tal como estabelecido no anexo II e nas declarações e compromissos oficiais constantes dos documentos enumerados nos anexos I e III a VII.

3. Para efeitos do n.º 1, os dados pessoais são transferidos ao abrigo do Escudo de Proteção da Privacidade [União Europeia]-EUA sempre que sejam transferidos da União para organizações nos Estados Unidos que constem da "lista do Escudo de Proteção da Privacidade", mantida e disponibilizada ao público pelo Department of Commerce dos EUA, em conformidade com as secções I e III dos princípios estabelecidos no anexo II.»

47 O anexo II da Decisão BPD, sob a epígrafe «Princípios do quadro do Escudo de Proteção da Privacidade [União Europeia]-EUA emitidos pelo Department of Commerce dos EUA», prevê, no seu ponto I.5, que a adesão a estes princípios pode ser limitada, nomeadamente, «na medida necessária para observar requisitos de segurança nacional, [de] interesse público ou [de] execução legal».

48 O anexo III desta decisão contém uma carta de John Kerry, então Secretary of State (secretário de Estado, Estados Unidos), dirigida à comissária responsável pela Justiça, Consumidores e Igualdade de Género, de 7 de julho de 2016, à qual está junta, como anexo A, um memorando intitulado «Mecanismo do Mediador para o Escudo de Proteção da Privacidade [União Europeia]-EUA Relativamente à informação de origem eletromagnética», que contém a seguinte passagem:

«Reconhecendo a importância do quadro do Escudo de Proteção da Privacidade [União Europeia]-EUA, o presente memorando estabelece o processo de implementação de um novo mecanismo, em conformidade com a Presidential Policy Directive 28 (PPD-28), no que se refere à informação de origem eletromagnética.

[…] O [p]residente Obama anunciou a emissão de uma nova diretiva presidencial — a PPD-28 — para "prescrever exatamente o que fazemos e o que não fazemos, no que diz respeito à nossa vigilância no estrangeiro".

A secção 4, alínea d), da PPD-28 exige que o [s]ecretário de Estado nomeie um "Senior Coordinator for International Information Technology Diplomacy" (coordenador superior) "para exercer a função de ponto de contacto para os governos estrangeiros que desejem manifestar preocupações relativamente às atividades de informação de origem eletromagnética realizadas pelos EUA".

[…]

1) [O coordenador superior] exercerá a função de Mediador para o Escudo de Proteção da Privacidade e […] trabalhará em estreita colaboração com os funcionários adequados de outros departamentos e organismos responsáveis pelo tratamento de pedidos em conformidade com a legislação e política aplicáveis dos Estados Unidos. O Mediador é independente do setor das informações. O Mediador responde diretamente perante o [s]ecretário de Estado, que assegurará que este desempenhe as suas funções de forma objetiva e isenta de influências indevidas que possa afetar a resposta a fornecer.

[…]»

49 O anexo VI da Decisão BPD contém uma carta do Gabinete do Diretor dos Serviços Nacionais de Informações (Office of the Director of National Intelligence) para o Department of Commerce [(Ministério do Comércio)] dos EUA e para a International Trade Administration [(Administração do Comércio Internacional)], de 21 de junho de 2016, na qual se precisa que a PPD-28 permite proceder a uma «recolha em larga escala […] de um volume relativamente elevado de informações ou dados de origem eletromagnética em circunstâncias em que o setor das informações não pode utilizar um identificador associado a um objetivo específico […] para centrar a recolha».

Litígio no processo principal e questões prejudiciais

50 M. Schrems, cidadão austríaco residente na Áustria, é utilizador da rede social Facebook (a seguir «Facebook»), desde 2008.

51 Qualquer pessoa que resida no território da União e que pretenda utilizar o Facebook é obrigada, 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 no território dos Estados Unidos, onde são objeto de tratamento.

52 Em 25 de junho de 2013, M. Schrems apresentou ao Comissário uma queixa em que lhe pedia, em substância, que proibisse a Facebook Ireland de transferir os seus dados pessoais para os Estados Unidos, alegando 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. Esta queixa foi arquivada, com o fundamento, nomeadamente, de que a Comissão tinha constatado, na sua Decisão 2000/520, que os Estados Unidos asseguravam um nível de proteção adequado.

53 A High Court (Tribunal Superior, Irlanda), para a qual M. Schrems interpôs recurso do arquivamento da sua queixa, submeteu ao Tribunal de Justiça um pedido de decisão prejudicial relativo à interpretação e à validade da Decisão 2000/520. Por Acórdão de 6 de outubro de 2015, Schrems (C-362/14, EU:C:2015:650), o Tribunal de Justiça declarou essa decisão inválida.

54 Na sequência desse acórdão, o órgão jurisdicional de reenvio anulou o arquivamento da queixa de M. Schrems e remeteu-a ao Comissário. No âmbito do inquérito aberto por este último, a Facebook Ireland explicou que grande parte dos dados pessoais era transferida para a Facebook Inc. com base nas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT. Tendo em conta estes elementos, o Comissário convidou M. Schrems a reformular a sua queixa.

55 Na sua queixa assim reformulada, apresentada em 1 de dezembro de 2015, M. Schrems alegou, nomeadamente, que o direito americano impõe à Facebook Inc. que coloque os dados pessoais que para ela são transferidos à disposição das autoridades americanas, como a National Security Agency (NSA) e o Federal Bureau of Investigation (FBI). Sustentou que, uma vez que estes dados são utilizados, no âmbito de diferentes programas de vigilância, de forma incompatível com os artigos 7.º, 8.º e 47.º da Carta, a Decisão CPT não pode justificar a transferência dos referidos dados para os Estados Unidos. Nestas condições, M. Schrems pediu ao Comissário que proibisse ou suspendesse a transferência dos seus dados pessoais para a Facebook Inc.

56 Em 24 de maio de 2016, o Comissário publicou um «projeto de decisão» que resumia as conclusões provisórias da sua investigação. Nesse projeto, considerou provisoriamente que os dados pessoais dos cidadãos da União transferidos para os Estados Unidos correm o risco de ser consultados e tratados, pelas autoridades americanas, de forma incompatível com os artigos 7.º e 8.º da Carta e que o direito dos Estados Unidos não oferece a esses cidadãos vias de recurso compatíveis com o artigo 47.º da Carta. O Comissário considerou que as cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT não são suscetíveis de sanar esse vício, na medida em que apenas conferem aos titulares dos dados direitos contratuais contra o exportador e o importador dos dados, sem, todavia, vincular as autoridades americanas.

57 Considerando que, nestas condições, a queixa reformulada de M. Schrems suscitava a questão da validade da Decisão CPT, o Comissário pediu à High Court (Tribunal Superior), em 31 de maio de 2016, com base na jurisprudência resultante do Acórdão de 6 de outubro de 2015, Schrems (C-362/14, EU:C:2015:650, n.º 65), que interrogasse o Tribunal de Justiça sobre esta questão. Por Decisão de 4 de maio de 2018, a High Court (Tribunal Superior) submeteu ao Tribunal de Justiça o presente reenvio prejudicial.

58 A High Court (Tribunal Superior) anexou a este reenvio prejudicial um acórdão, proferido em 3 de outubro de 2017, no qual tinha exposto o resultado da análise das provas que lhe foram apresentadas no âmbito do processo nacional, processo em que participou o Governo americano.

59 Nesse acórdão, ao qual o pedido de decisão prejudicial se refere várias vezes, o órgão jurisdicional de reenvio salientou que, por princípio, tem não só o direito mas também a obrigação de examinar todos os factos e argumentos invocados perante si, para decidir, com fundamento nesses factos e argumentos, se é ou não necessário um reenvio prejudicial. De qualquer modo, estava obrigado a ter em conta as eventuais alterações de direito ocorridas entre a interposição do recurso e a audiência realizada perante si. Esse órgão jurisdicional precisou que, no âmbito do processo principal, a sua própria apreciação não se limita aos fundamentos de invalidade invocados pelo Comissário, podendo igualmente apreciar oficiosamente outros fundamentos de invalidade e, com base nestes, proceder a um reenvio prejudicial.

60 Segundo as constatações que figuram no referido acórdão, as atividades de informação das autoridades americanas no que respeita aos dados pessoais transferidos para os Estados Unidos baseiam-se, nomeadamente, na secção 702 da FISA e no E.O. 12333.

61 No que se refere à secção 702 da FISA, o órgão jurisdicional de reenvio precisa, no mesmo acórdão, que esta disposição permite ao procurador-geral e ao diretor dos Serviços Nacionais de Informações autorizarem conjuntamente, após aprovação do FISC, com o fim de obter «informações em matéria de informação externa», a vigilância de nacionais não americanos que se encontram fora do território

dos Estados Unidos e serve, nomeadamente, de fundamento aos programas de vigilância PRISM e UPSTREAM. No âmbito do programa PRISM, os fornecedores de serviços de Internet são obrigados, segundo as constatações daquele órgão jurisdicional, a fornecer à NSA todas as comunicações enviadas e recebidas por um «seletor», sendo uma parte dessas comunicações transmitida também ao FBI e à Central Intelligence Agency (CIA) (Agência Central de Informações).

62 Quanto ao programa UPSTREAM, o referido órgão jurisdicional constatou que, no âmbito deste programa, as empresas de telecomunicações que exploram a «dorsal» da Internet — isto é, a rede de cabos, comutadores e rotores — são obrigadas a permitir à NSA copiar e filtrar os fluxos de tráfego na Internet a fim de recolher comunicações enviadas ou recebidas por ou relativas a um nacional não americano visado por um «seletor». No âmbito do mesmo programa, segundo as conclusões desse mesmo órgão jurisdicional, a NSA tem acesso tanto aos metadados como ao conteúdo das comunicações em causa.

63 No que respeita ao E.O. 12333, o órgão jurisdicional de reenvio observa que este permite à NSA aceder a dados «em trânsito» para os Estados Unidos, acedendo aos cabos submarinos colocados no fundo do Atlântico, bem como recolher e conservar esses dados antes de chegarem aos Estados Unidos e serem aí sujeitos às disposições da FISA. Precisa que as atividades baseadas no E.O. 12333 não são reguladas pela lei.

64 Quanto aos limites impostos às atividades de informação, o órgão jurisdicional de reenvio põe a tónica no facto de as pessoas não americanas estarem unicamente abrangidas pela PPD-28 e de esta se limitar a indicar que as atividades de informação deviam ser «tão personalizadas quanto possível» (*as tailored as feasible*). Com base nas suas constatações, o referido órgão jurisdicional considera que os Estados Unidos procedem a um tratamento de dados em massa, sem assegurarem uma proteção substancialmente equivalente à garantida pelos artigos 7.º e 8.º da Carta.

65 Quanto à proteção jurisdicional, esse mesmo órgão jurisdicional refere que os cidadãos da União não têm acesso aos mesmos recursos de que os nacionais americanos dispõem contra os tratamentos de dados pessoais pelas autoridades americanas, uma vez que a Quarta Emenda da Constitution of the United States (Constituição dos Estados Unidos), que constitui, no direito americano, a proteção mais importante contra a vigilância ilegal, é inaplicável aos cidadãos da União. A este respeito, o órgão jurisdicional de reenvio precisa que os recursos que permanecem à disposição destes últimos esbarram com importantes obstáculos, em particular a obrigação — em seu entender, excessivamente difícil de satisfazer — de demonstrar a sua legitimidade processual. Por outro lado, segundo as constatações desse órgão jurisdicional, as atividades da NSA baseadas no E.O. 12333 não são objeto de fiscalização jurisdicional e não são suscetíveis de recursos judiciais. Por último, o referido órgão jurisdicional considera que, na medida em que, no seu entender, o Mediador para o Escudo de Proteção da Privacidade não constitui um tribunal, na aceção do artigo 47.º da Carta, o direito americano não garante aos cidadãos da União um nível de proteção substancialmente equivalente ao garantido pelo direito fundamental consagrado neste artigo.

66 No seu pedido de decisão prejudicial, o órgão jurisdicional de reenvio precisa ainda que as partes no processo principal se opõem, nomeadamente, quanto à questão da aplicabilidade do direito da União a transferências, para um país terceiro, de dados pessoais suscetíveis de serem tratados pelas autoridades desse país, nomeadamente, para efeitos de segurança nacional, e quanto aos elementos a tomar em consideração para efeitos da apreciação do nível de proteção adequado, assegurado pelo referido país. Em particular, esse órgão jurisdicional salienta que, segundo a Facebook Ireland, as constatações da Comissão relativas ao caráter adequado do nível de proteção assegurado por um país terceiro, como as que figuram na Decisão BPD, vinculam as autoridades de controlo igualmente no contexto de uma transferência de dados pessoais baseada nas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT.

67 No que respeita a estas cláusulas-tipo de proteção de dados, o referido órgão jurisdicional interroga-se sobre se a Decisão CPT pode ser considerada válida, apesar de, segundo esse mesmo órgão jurisdicional, as referidas cláusulas não serem vinculativas para as autoridades estatais do país terceiro em causa e, por conseguinte, não serem suscetíveis de sanar uma eventual inexistência de nível de proteção adequado nesse país. A este respeito, considera que a possibilidade, reconhecida às autoridades competentes dos Estados-Membros pelo artigo 4.º, n.º 1, alínea a), da Decisão 2010/87, na sua versão anterior à entrada em vigor da Decisão de Execução 2016/2297, de proibir as transferências de dados pessoais para um país terceiro que imponha ao importador obrigações incompatíveis com as garantias constantes dessas mesmas cláusulas, demonstra que o estado do direito do país terceiro pode justificar a proibição de uma transferência de dados, mesmo que esta seja efetuada com base nas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT, e, portanto, mostra que estas podem ser insuficientes para assegurar uma proteção adequada. Não obstante, o órgão jurisdicional de reenvio interroga-se sobre o alcance do poder do Comissário para proibir uma transferência de dados baseada nessas cláusulas, embora considere que um poder discricionário não pode ser suficiente para assegurar uma proteção adequada.

68 Foi nestas condições que a High Court (Tribunal Superior) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Em circunstâncias nas quais uma empresa privada transfere, com base na [Decisão CPT], de um Estado-Membro da [União] para uma empresa privada num país terceiro, para fins comerciais, dados pessoais que podem ser tratados posteriormente pelas autoridades do país terceiro não só para fins de segurança nacional mas também para efeitos da [manutenção da ordem pública] e da administração dos assuntos externos do país terceiro, [é] o direito da [União], [incluindo a Carta,] aplicável à transferência dos dados, [não obstante as] disposições do artigo 4.º, n.º 2, TUE relativas à segurança nacional e as disposições do artigo 3.º, n.º 2, primeiro travessão, da [Diretiva 95/46] [relativas] à segurança pública, [à] defesa e [à] segurança do Estado?

2) a) Para efeitos da Diretiva [95/46], ao determinar se constitui violação dos direitos de uma pessoa [a transferência de] dados ao abrigo, a partir da [União] para um país terceiro no qual esses dados podem ser posteriormente tratados para fins de segurança nacional, o elemento de referência pertinente é:
   i) a Carta, o [Tratado UE], o [Tratado FUE], a Diretiva [95/46], a [Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, assinada em Roma, em 4 de novembro de 1950] (ou qualquer outra disposição do direito da União), ou;
   ii) a legislação nacional de um ou mais Estados-Membros?
   b) Se o elemento de referência pertinente for o referido [em ii)], devem ser igualmente incluídas nesse elemento as práticas seguidas [em matéria de] segurança nacional num ou em vários Estados-Membros?

3) Ao avaliar se um país terceiro assegura o nível de proteção exigido pelo direito da União para transferir dados pessoais para esse país, para efeitos do artigo 26.º da Diretiva [95/46], deve o nível de proteção no país terceiro ser avaliado por referência:
   a) Às regras aplicáveis no país terceiro decorrentes da sua legislação interna ou dos [seus] compromissos internacionais […] e à prática seguida para garantir o cumprimento dessas regras, [incluindo] as regras profissionais e as medidas de segurança aplicadas no país terceiro;

   ou

   b) Às regras referidas na alínea a), juntamente com as práticas administrativas, regulamentares e de [aplicação da lei], e as medidas de proteção, […] os procedimentos, protocolos [e] mecanismos de supervisão [bem como as] vias de recurso extrajudiciais aplicáveis no país terceiro?

4) Constitui violação dos direitos das pessoas, previstos nos artigos 7.º e/ou 8.º da Carta, a transferência de dados pessoais da [União] para os EUA ao abrigo da Decisão [CPT], tendo em conta os factos apurados pela High Court [(Tribunal Superior)] em relação à lei dos EUA?

5) Tendo em conta os factos apurados pela High Court [(Tribunal Superior)] em relação à lei dos EUA, no caso de serem transferidos dados pessoais da [União] para os EUA ao abrigo da Decisão [CPT]:
   a) O nível de proteção conferido pelos EUA respeita o conteúdo essencial do direito das pessoas a [uma ação] judicial [por] violação dos seus direitos [à confidencialidade] dos dados, [garantido pelo] artigo 47.º da Carta?

   Se a resposta à alínea a) for afirmativa:
   b) As limitações impostas pela legislação dos EUA ao direito das pessoas a [uma ação] judicial no contexto da segurança nacional dos EUA são proporcionadas, na aceção do artigo 52.º da Carta, e não excedem o que é necessário numa sociedade democrática para fins de segurança nacional?

6) a) Qual é, […] à luz das disposições da Diretiva [95/46] e, em especial, dos [seus] artigos 25.º e 26.º, interpretados à luz da Carta, o nível de proteção que deve ser concedido aos dados pessoais transferidos para um país terceiro ao abrigo de cláusulas contratuais-tipo estipuladas em conformidade com uma decisão da Comissão[, a título do artigo 26.º, n.º 4, da Diretiva 95/46]?
   b) Quais são os elementos a ter em conta, ao avaliar se o nível de proteção concedido aos dados transferidos para um país terceiro ao abrigo da Decisão [CPT] cumpre as exigências da Diretiva [95/46] e da Carta?

7) O facto de as cláusulas contratuais-tipo serem aplicáveis ao exportador de dados e ao importador de dados, mas não serem vinculativas para as autoridades nacionais de um país terceiro, que podem exigir que o importador de dados disponibilize [aos] seus serviços de segurança, para […] tratamento posterior, os dados pessoais transferidos ao abrigo das cláusulas previstas na Decisão [CPT], [exclui] que [essas] cláusulas [ofereçam as] garantias de proteção adequadas previstas no artigo 26.º, n.º 2, da Diretiva [95/46]?

8) Se um importador de dados de um país terceiro estiver sujeito a leis de vigilância que, na opinião de uma autoridade de [controlo], estejam em conflito com as cláusulas [contratuais-tipo] ou com os artigos 25.º e 26.º da Diretiva [95/46] e/ou com a Carta, é uma autoridade de [controlo] obrigada a exercer os seus poderes de execução previstos no artigo 28.º, n.º 3, da Diretiva [95/46] para suspender os fluxos de dados, ou o exercício desses poderes limita-se apenas a casos excecionais, à luz do considerando 11 da [Decisão CPT], ou pode uma autoridade de [controlo] utilizar o seu poder discricionário para não suspender esses fluxos de dados?

9) a) Para efeitos do artigo 25.º, n.º 6, da Diretiva [95/46], constitui a Decisão [BPD] uma [declaração] de aplicação geral que é vinculativa para as autoridades de [controlo] e para os tribunais dos Estados-Membros, [segundo a qual] os Estados Unidos[, em razão do seu direito interno ou dos seus compromissos internacionais, garantem] um nível de proteção adequado, na aceção do artigo 25.º, n.º 2, da Diretiva [95/46]?
   b) Se assim não for, [qual é a eventual relevância] da Decisão [BPD] na avaliação realizada sobre a adequação [das garantias oferecidas] aos dados transferidos para os Estados Unidos em conformidade com a Decisão [2010/87]?

10) Tendo em conta as considerações da High Court [(Tribunal Superior)] relativas à legislação dos EUA, constitui a previsão de um Mediador para o Escudo de Proteção da Privacidade a que se refere o [anexo III] da Decisão [BPD], quando considerada em conjugação com o regime vigente

nos Estados Unidos, uma garantia de que este país oferece uma via de recurso compatível com o artigo 47.º da Carta […] àqueles cujos dados pessoais são transferidos para os EUA ao abrigo da Decisão [CPT]?

11) A Decisão [CPT] viola os artigos 7.º, 8.º ou 47.º da Carta?»

Quanto à admissibilidade do pedido de decisão prejudicial

69 A Facebook Ireland e os Governos alemão e do Reino Unido alegam que o pedido de decisão prejudicial é inadmissível.

70 No que se refere à exceção suscitada pela Facebook Ireland, esta sociedade observa que as disposições da Diretiva 95/46 em que se baseiam as questões prejudiciais foram revogadas pelo RGPD.

71 A este respeito, embora seja verdade que, por força do artigo 94.º, n.º 1, do RGPD, a Diretiva 95/46 foi revogada com efeitos a partir de 25 de maio de 2018, ainda estava em vigor aquando da formulação, em 4 de maio de 2018, do presente pedido de decisão prejudicial, que deu entrada no Tribunal de Justiça em 9 de maio de 2018. Além disso, o artigo 3.º, n.º 2, primeiro travessão, os artigos 25.º e 26.º e o artigo 28.º, n.º 3, da Diretiva 95/46, aos quais se referem as questões prejudiciais, foram reproduzidos, em substância, respetivamente, no artigo 2.º, n.º 2, e nos artigos 45.º, 46.º e 58.º do RGPD. Por outro lado, há que recordar que o Tribunal de Justiça tem por missão interpretar todas as disposições do direito da União de que os órgãos jurisdicionais nacionais necessitem para decidir dos litígios que lhes são submetidos, ainda que essas disposições não sejam expressamente referidas nas questões que lhe são apresentadas por esses órgãos jurisdicionais (Acórdão de 2 de abril de 2020, Ruska Federacija, C-897/19 PPU, EU:C:2020:262, n.º 43 e jurisprudência referida). Por estes diferentes motivos, a circunstância de o órgão jurisdicional de reenvio ter formulado as questões prejudiciais referindo-se unicamente às disposições da Diretiva 95/46 não pode implicar a inadmissibilidade do presente pedido de decisão prejudicial.

72 Por seu turno, o Governo alemão baseia a sua exceção de inadmissibilidade na circunstância, por um lado, de o Comissário apenas ter apresentado dúvidas, e não uma opinião definitiva, quanto à questão da validade da Decisão CPT e, por outro, de o órgão jurisdicional de reenvio não ter verificado se M. Schrems tinha indubitavelmente dado o seu consentimento às transferências de dados em causa no processo principal, o que, a ser o caso, teria por efeito tornar inútil uma resposta a esta questão. Por último, segundo o Governo do Reino Unido, as questões prejudiciais têm caráter hipotético, uma vez que esse órgão jurisdicional não constatou que esses dados tinham sido efetivamente transferidos com base na referida decisão.

73 Resulta de jurisprudência constante do Tribunal de Justiça que o juiz nacional, a quem foi submetido o litígio e que deve assumir a responsabilidade pela decisão judicial a tomar, tem competência exclusiva para apreciar, tendo em conta as especificidades do processo, tanto a necessidade de uma decisão prejudicial para poder proferir a sua decisão como a pertinência das questões que submete ao Tribunal de Justiça. Consequentemente, desde que as questões submetidas sejam relativas à interpretação ou à validade de uma regra do direito da União, o Tribunal de Justiça é, em princípio, obrigado a pronunciar-se. Daqui se conclui que as questões submetidas pelos órgãos jurisdicionais nacionais gozam de uma presunção de pertinência. O Tribunal de Justiça só pode recusar pronunciar-se sobre uma questão prejudicial submetida por um órgão jurisdicional nacional se se afigurar que a interpretação solicitada não tem nenhuma relação com a realidade ou com o objeto do litígio no processo principal, se o problema for hipotético ou ainda se o Tribunal de Justiça não dispuser dos elementos de facto e de direito necessários para dar uma resposta útil às referidas questões (Acórdãos de 16 de junho de 2015, Gauweiler e o., C-62/14, EU:C:2015:400, n.ºs 24 e 25; de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 45; e de 19 de dezembro de 2019, Dobersberger, C-16/18, EU:C:2019:1110, n.ºs 18 e 19).

74 No caso vertente, o pedido de decisão prejudicial contém elementos de facto e de direito suficientes para se compreender o alcance das questões prejudiciais. Além disso, e sobretudo, nenhum elemento dos autos de que o Tribunal de Justiça dispõe permite considerar que a interpretação solicitada do direito da União não tem relação com a realidade ou com o objeto do litígio no processo principal ou que é de natureza hipotética, nomeadamente devido ao facto de a transferência dos dados pessoais em causa no processo principal se basear no consentimento explícito do titular dos dados a essa transferência, e não na Decisão CPT. Com efeito, segundo as indicações que figuram nesse pedido, a Facebook Ireland reconheceu que transfere para a Facebook Inc. os dados pessoais dos seus utilizadores que residem na União e que grande parte dessas transferências, cuja licitude M. Schrems contesta, é efetuada com base nas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT.

75 Por outro lado, é irrelevante para a admissibilidade do presente pedido prejudicial que o Comissário não tenha expressado uma opinião definitiva sobre a validade daquela decisão, uma vez que o órgão jurisdicional de reenvio considera que a resposta às questões prejudiciais relativas à interpretação e à validade de regras do direito da União é necessária para a resolução do litígio no processo principal.

76 Daqui resulta que o pedido de decisão prejudicial é admissível.

Quanto às questões prejudiciais

77 A título preliminar, há que recordar que o presente pedido de decisão prejudicial tem origem numa queixa apresentada por M. Schrems, destinada a que o Comissário ordene a suspensão ou a proibição, para o futuro, da transferência dos seus dados pessoais pela Facebook Ireland para a Facebook Inc. Ora, embora as questões prejudiciais se refiram às disposições da Diretiva 95/46, é pacífico que o Comissário ainda não tinha adotado uma decisão final sobre essa queixa quando esta diretiva foi revogada e substituída pelo RGPD, com efeitos em 25 de maio de 2018.

78 Esta inexistência de decisão nacional distingue a situação em causa no processo principal das situações que deram origem aos Acórdãos de 24 de setembro de 2019, Google (Âmbito territorial da supressão de referências) (C-507/17, EU:C:2019:772), e de 1 de outubro de 2019, Planet49 (C-673/17, EU:C:2019:801), nas quais estavam em causa decisões adotadas antes da revogação da referida diretiva.

79 Como tal, há que responder às questões prejudiciais à luz das disposições do RGPD, e não das da Diretiva 95/46.

Quanto à primeira questão

80 Com a sua primeira questão, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 2.º, n.º 1, e o artigo 2.º, n.º 2, alíneas a), b) e d), do RGPD, lidos em conjugação com o artigo 4.º, n.º 2, TUE, devem ser interpretados no sentido de que está abrangida pelo âmbito de aplicação deste regulamento uma transferência de dados pessoais efetuada por um operador económico estabelecido num Estado-Membro para outro operador económico estabelecido num país terceiro, quando, durante ou na sequência dessa transferência, esses dados são suscetíveis de ser tratados pelas autoridades desse país terceiro para efeitos de segurança pública, de defesa e de segurança do Estado.

81 A este respeito, importa salientar, antes de mais, que a disposição contida no artigo 4.º, n.º 2, TUE, segundo a qual, na União, a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro, respeita unicamente aos Estados-Membros da União. Por conseguinte, esta disposição não é pertinente, no caso vertente, para interpretar o artigo 2.º, n.º 1, e o artigo 2.º, n.º 2, alíneas a), b) e d), do RGPD.

82 Nos termos do seu artigo 2.º, n.º 1, o RGPD aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados. O artigo 4.º, ponto 2, deste regulamento define o conceito de «tratamento» como «uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados», e refere, a título exemplificativo, «a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização», sem distinguir consoante essas operações sejam realizadas na União ou tenham uma ligação com um país terceiro. Além disso, o referido regulamento sujeita as transferências de dados pessoais para países terceiros a regras especiais que figuram no seu capítulo V, sob a epígrafe «Transferências de dados pessoais para países terceiros ou organizações internacionais», e confere, além disso, às autoridades de controlo, poderes específicos para esse efeito, que figuram no artigo 58.º, n.º 2, alínea j), do mesmo regulamento.

83 Daqui decorre que a operação que consiste na transferência de dados pessoais de um Estado-Membro para um país terceiro constitui, enquanto tal, um tratamento de dados pessoais na aceção do artigo 4.º, ponto 2, do RGPD, efetuado no território de um Estado-Membro, tratamento ao qual esse regulamento é aplicável por força do seu artigo 2.º, n.º 1 [v., por analogia, no que respeita ao artigo 2.º, alínea b), e ao artigo 3.º, n.º 1, da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 45 e jurisprudência referida].

84 No que respeita à questão de saber se se pode considerar que tal operação está excluída do âmbito de aplicação do RGPD por força do seu artigo 2.º, n.º 2, importa recordar que esta disposição prevê exceções ao âmbito de aplicação desse regulamento, conforme definido no seu artigo 2.º, n.º 1, e que essas exceções devem ser objeto de interpretação estrita (v., por analogia, no que respeita ao artigo 3.º, n.º 2, da Diretiva 95/46, Acórdão de 10 de julho de 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, n.º 37 e jurisprudência referida).

85 No caso vertente, uma vez que a transferência de dados pessoais em causa no processo principal é efetuada pela Facebook Ireland para a Facebook Inc., a saber, entre duas pessoas coletivas, essa transferência não está abrangida pelo artigo 2.º, n.º 2, alínea c), do RGPD, que visa o tratamento de dados efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas. A referida transferência também não está abrangida pelo âmbito de aplicação das exceções que figuram no artigo 2.º, n.º 2, alíneas a), b) e d), deste regulamento, uma vez que as atividades aí referidas a título de exemplo são, em qualquer caso, atividades próprias dos Estados ou das autoridades estatais, alheias aos domínios de atividade dos particulares (v., por analogia, no que respeita ao artigo 3.º, n.º 2, da Diretiva 95/46, Acórdão de 10 de julho de 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, n.º 38 e jurisprudência referida).

86 Ora, a possibilidade de os dados pessoais transferidos entre dois operadores económicos para fins comerciais sofrerem, no decurso ou na sequência da transferência, um tratamento para efeitos de segurança pública, de defesa e de segurança do Estado, pelas autoridades do país terceiro em causa, não pode excluir a referida transferência do âmbito de aplicação do RGPD.

87 Além disso, ao impor expressamente à Comissão, quando esta avalia o caráter adequado do nível de proteção oferecido por um país terceiro, a obrigação de ter em conta, nomeadamente, «a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados», a própria redação do artigo 45.º, n.º 2, alínea a), deste regulamento evidencia o facto de que o eventual tratamento dos dados em causa, por um país terceiro, para efeitos de segurança pública, de defesa e de segurança do Estado, não põe em causa a aplicabilidade do referido regulamento à transferência.

88 Daqui decorre que essa transferência não pode escapar ao âmbito de aplicação do RGPD pelo facto de os dados em causa serem suscetíveis de ser tratados, no decurso ou na sequência dessa transferência, pelas autoridades do país terceiro em causa, para efeitos de segurança pública, de defesa e de segurança do Estado.

89 Por conseguinte, há que responder à primeira questão que o artigo 2.º, n.ºs 1 e 2, do RGPD deve ser interpretado no sentido de que está abrangida pelo âmbito de aplicação deste regulamento uma transferência de dados pessoais efetuada para fins comerciais por um operador económico estabelecido num Estado-Membro para outro operador económico estabelecido num país terceiro, não obstante o facto de, no decurso ou na sequência dessa transferência, esses dados serem suscetíveis de ser tratados pelas autoridades do país terceiro em causa para efeitos de segurança pública, de defesa e de segurança do Estado.

Quanto à segunda, terceira e sexta questões

90 Com a sua segunda, terceira e sexta questões, o órgão jurisdicional de reenvio interroga o Tribunal de Justiça, em substância, sobre o nível de proteção exigido pelo artigo 46.º, n.º 1, e pelo artigo 46.º, n.º 2, alínea c), do RGPD no âmbito de uma transferência de dados pessoais para um país terceiro com base nas cláusulas-tipo de proteção de dados. Em particular, este órgão jurisdicional pede ao Tribunal de Justiça que precise os elementos a tomar em consideração para determinar se esse nível de proteção é assegurado no contexto dessa transferência.

91 No que respeita ao nível de proteção exigido, resulta de uma leitura conjugada destas disposições que, não tendo sido uma decisão de adequação adotada nos termos do artigo 45.º, n.º 3, deste regulamento, o responsável pelo tratamento ou o subcontratante só pode transferir dados pessoais para um país terceiro se tiver apresentado «garantias adequadas» e na condição de os titulares dos dados «gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes», podendo essas garantias adequadas ser previstas, nomeadamente, por cláusulas-tipo de proteção de dados adotadas pela Comissão.

92 Embora o artigo 46.º do RGPD não especifique a natureza das exigências que decorrem desta referência às «garantias adequadas», aos «direitos oponíveis» e às «medidas jurídicas corretivas eficazes», importa salientar que este artigo figura no capítulo V deste regulamento e, portanto, deve ser lido à luz do artigo 44.º do dito regulamento, sob a epígrafe «Princípio geral das transferências», que estabelece que «[t]odas as disposições [deste capítulo] são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido [pelo mesmo] regulamento». Este nível de proteção deve, por conseguinte, ser garantido independentemente da disposição daquele capítulo com base na qual é efetuada uma transferência de dados pessoais para um país terceiro.

93 Com efeito, como salientou o advogado-geral no n.º 117 das suas conclusões, as disposições do capítulo V do RGPD visam assegurar a continuidade do elevado nível dessa proteção em caso de transferência de dados pessoais para um país terceiro, em conformidade com o objetivo precisado no considerando 6 desse regulamento.

94 O artigo 45.º, n.º 1, primeiro período, do RGPD prevê que uma transferência de dados pessoais para um país terceiro pode ser autorizada através de uma decisão adotada pela Comissão, segundo a qual esse país terceiro, um território ou um ou mais setores específicos desse país terceiro assegura um nível de proteção adequado. A este respeito, sem exigir que o país terceiro em causa garanta um nível de proteção idêntico ao garantido na ordem jurídica da União, a expressão «nível de proteção adequado» deve ser entendida, como confirma o considerando 104 deste regulamento, 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 dos direitos fundamentais substancialmente equivalente ao garantido na União por força do referido regulamento, lido à luz da

Carta. Com efeito, na falta de uma exigência desta natureza, o objetivo mencionado no número anterior seria ignorado (v., por analogia, no que respeita ao artigo 25.º, n.º 6, da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 73).

95 Neste contexto, o considerando 107 do RGPD enuncia que, quando «um país terceiro, um território ou um setor específico de um país terceiro […] deixou de assegurar um nível adequado de proteção de dados […], deverá ser proibida a transferência de dados pessoais para esse país terceiro […], a menos que sejam cumpridos os requisitos constantes [desse regulamento] relativos a transferências sujeitas a garantias adequadas […]». Para este efeito, o considerando 108 do referido regulamento precisa que, na falta de uma decisão de adequação, as garantias adequadas que o responsável pelo tratamento ou o subcontratante deve adotar em conformidade com o artigo 46.º, n.º 1, do mesmo regulamento devem «colmatar a insuficiência da proteção de dados no país terceiro» para «assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União».

96 Daqui resulta, como salientou o advogado-geral no n.º 115 das suas conclusões, que essas garantias adequadas devem ser de natureza a assegurar que as pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas-tipo de proteção de dados beneficiam, como no âmbito de uma transferência baseada numa decisão de adequação, de um nível de proteção substancialmente equivalente ao garantido na União.

97 O órgão jurisdicional de reenvio interroga-se igualmente sobre a questão de saber se esse nível de proteção substancialmente equivalente ao garantido na União deve ser determinado à luz do direito da União, nomeadamente dos direitos garantidos pela Carta, e/ou à luz dos direitos fundamentais consagrados na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (a seguir «CEDH»), ou ainda à luz do direito nacional dos Estados-Membros.

98 A este respeito, importa recordar que, embora, como confirma o artigo 6.º, n.º 3, TUE, os direitos fundamentais consagrados pela CEDH façam parte do direito da União, enquanto princípios gerais, e embora o artigo 52.º, n.º 3, da Carta disponha que os direitos nela contidos que correspondam a direitos garantidos pela CEDH têm o mesmo sentido e o mesmo alcance que os que lhes são conferidos pela referida convenção, esta não constitui, enquanto a União não aderir à mesma, um instrumento jurídico formalmente integrado na ordem jurídica da União (Acórdãos de 26 de fevereiro de 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, n.º 44 e jurisprudência referida, e de 20 de março de 2018, Menci, C-524/15, EU:C:2018:197, n.º 22).

99 Nestas condições, o Tribunal de Justiça declarou que a interpretação do direito da União e o exame da validade dos atos da União devem ser realizados à luz dos direitos fundamentais garantidos pela Carta (v., por analogia, Acórdão de 20 de março de 2018, Menci, C-524/15, EU:C:2018:197, n.º 24).

100 Além do mais, é jurisprudência constante que a validade das disposições do direito da União e, na falta de uma remissão expressa para o direito nacional dos Estados-Membros, a sua interpretação não podem ser apreciadas à luz desse direito nacional, mesmo que de nível constitucional, em particular dos direitos fundamentais conforme formulados na sua Constituição nacional (v., neste sentido, Acórdãos de 17 de dezembro de 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, n.º 3; de 13 de dezembro de 1979, Hauer, 44/79, EU:C:1979:290, n.º 14; e de 18 de outubro de 2016, Nikiforidis, C-135/15, EU:C:2016:774, n.º 28 e jurisprudência referida).

101 Conclui-se que, uma vez que, por um lado, uma transferência de dados pessoais como a que está em causa no processo principal, efetuada para fins comerciais por um operador económico estabelecido num Estado-Membro, com destino a outro operador económico estabelecido num país terceiro, está abrangida, como resulta da resposta à primeira questão, pelo âmbito de aplicação do RGPD e que, por outro, este regulamento visa, nomeadamente, como resulta do seu considerando 10, assegurar um nível de proteção coerente e elevado das pessoas singulares na União e, para o efeito, assegurar em toda a

União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais dessas pessoas no que diz respeito ao tratamento de dados pessoais, o nível de proteção dos direitos fundamentais exigido pelo artigo 46.º, n.º 1, do referido regulamento deve ser determinado com base nas disposições do mesmo regulamento, lidas à luz dos direitos fundamentais garantidos pela Carta.

102 O órgão jurisdicional de reenvio pretende ainda saber quais os elementos que devem ser tomados em consideração para determinar o caráter adequado do nível de proteção no contexto de uma transferência de dados pessoais para um país terceiro com base em cláusulas-tipo de proteção de dados adotadas ao abrigo do artigo 46.º, n.º 2, alínea c), do RGPD.

103 A este respeito, embora essa disposição não enumere os diferentes elementos a ter em conta para avaliar o caráter adequado do nível de proteção a respeitar no âmbito dessa transferência, o artigo 46.º, n.º 1, desse regulamento precisa que os titulares dos dados devem beneficiar de garantias adequadas e gozar de direitos oponíveis e de medidas jurídicas corretivas eficazes.

104 A avaliação exigida, para esse efeito, no contexto dessa transferência deve, nomeadamente, ter em consideração tanto as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais transferidos, os elementos pertinentes do sistema jurídico deste país terceiro. Quanto a este último aspeto, os elementos que importa tomar em consideração no contexto do artigo 46.º do referido regulamento correspondem aos enunciados, de maneira não exaustiva, no seu artigo 45.º, n.º 2.

105 Por conseguinte, há que responder à segunda, terceira e sexta questões que o artigo 46.º, n.º 1, e o artigo 46.º, n.º 2, alínea c), do RGPD devem ser interpretados no sentido de que as garantias adequadas, os direitos oponíveis e as medidas jurídicas corretivas eficazes, exigidos por estas disposições, devem assegurar que os direitos das pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas-tipo de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União por este regulamento, lido à luz da Carta. Para este efeito, a avaliação do nível de proteção assegurado no contexto dessa transferência deve, nomeadamente, ter em consideração tanto as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro, nomeadamente os enunciados no artigo 45.º, n.º 2, do referido regulamento.

Quanto à oitava questão

106 Com a sua oitava questão, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 58.º, n.º 2, alíneas f) e j), do RGPD deve ser interpretado no sentido de que a autoridade de controlo competente está obrigada a suspender ou a proibir uma transferência de dados pessoais para um país terceiro com base em cláusulas-tipo de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União, em particular pelos artigos 45.º e 46.º do RGPD e pela Carta, não pode ser assegurada, ou no sentido de que o exercício desses poderes está limitado a situações excecionais.

107 Em conformidade com o artigo 8.º, n.º 3, da Carta e com os artigos 51.º, n.º 1, e 57.º, n.º 1, alínea a), do RGPD, as autoridades nacionais de controlo estão encarregadas de fiscalizar o cumprimento das regras da União relativas à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais.

Por conseguinte, cada uma delas tem competência para verificar se uma transferência de dados pessoais do Estado-Membro dessa autoridade para um país terceiro respeita as exigências impostas por esse regulamento (v., por analogia, no que respeita ao artigo 28.º da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 47).

108 Decorre destas disposições que as autoridades de controlo têm por missão primordial fiscalizar a aplicação do RGPD e zelar pelo seu respeito. O exercício desta missão reveste particular importância no contexto de uma transferência de dados pessoais para um país terceiro, uma vez que, como resulta dos próprios termos do considerando 116 deste regulamento, «[s]empre que dados pessoais atravessarem fronteiras fora do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações». Nesta hipótese, como é precisado nesse mesmo considerando, «as autoridades de controlo podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras».

109 Além disso, por força do artigo 57.º, n.º 1, alínea f), do RGPD, cada autoridade de controlo está obrigada, no território respetivo, a tratar as reclamações que, em conformidade com o artigo 77.º, n.º 1, deste regulamento, qualquer pessoa tem o direito de apresentar quando considere que um tratamento de dados pessoais que lhe diga respeito constitui uma violação do referido regulamento, assim como a examinar o seu objeto na medida do necessário. A autoridade de controlo deve proceder ao tratamento de uma reclamação dessa natureza com toda a diligência exigida (v., por analogia, no que respeita ao artigo 25.º, n.º 6, da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 63).

110 O artigo 78.º, n.ºs 1 e 2, do RGPD reconhece a todas as pessoas o direito à ação judicial, nomeadamente quando a autoridade de controlo não trate a sua reclamação. O considerando 141 deste regulamento faz igualmente referência a este «direito a uma ação judicial efetiva, nos termos do artigo 47.º da Carta», no caso de essa autoridade de controlo «não tomar as iniciativas necessárias para proteger os [direitos dos titulares dos dados]».

111 Para tratar as reclamações apresentadas, o artigo 58.º, n.º 1, do RGPD investe cada autoridade de controlo de importantes poderes de investigação. Quando uma autoridade de controlo considere, no termo da sua investigação, que o titular dos dados que foram transferidos para um país terceiro não beneficia, neste país terceiro, de um nível de proteção adequado, está obrigada, em aplicação do direito da União, a reagir de forma apropriada, a fim de sanar a insuficiência verificada, independentemente da origem ou da natureza dessa insuficiência. A este respeito, o artigo 58.º, n.º 2, deste regulamento enumera os diferentes poderes de correção que a autoridade de controlo pode adotar.

112 Embora a escolha do meio adequado e necessário caiba à autoridade de controlo e esta deva efetuar essa escolha tomando em consideração todas as circunstâncias da transferência de dados pessoais em causa, esta autoridade não deixa de estar obrigada a cumprir com toda a diligência exigida a sua missão de zelar pelo pleno respeito do RGPD.

113 A este respeito, e como salientou igualmente o advogado-geral no n.º 148 das suas conclusões, a referida autoridade é obrigada, por força do artigo 58.º, n.º 2, alíneas f) e j), deste regulamento, a suspender ou a proibir a transferência de dados pessoais para um país terceiro, se considerar, à luz de todas as circunstâncias específicas dessa transferência, que as cláusulas-tipo de proteção de dados não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União não pode ser assegurada por outros meios, no caso de o responsável pelo tratamento ou o seu subcontratante estabelecidos na União não terem eles próprios suspendido ou posto termo à transferência.

114 A interpretação constante do número anterior não é infirmada pela argumentação do Comissário segundo a qual o artigo 4.º da Decisão 2010/87, na sua versão anterior à entrada em vigor da Decisão de Execução 2016/2297, lido à luz do considerando 11 desta decisão, limitava a certos casos excecionais o poder das autoridades de controlo de suspenderem ou de proibirem uma transferência de dados pessoais para um país terceiro. Com efeito, na sua versão resultante da Decisão de Execução 2016/2297, o artigo 4.º da Decisão CPT evoca o poder de que essas autoridades dispõem, atualmente por força do artigo 58.º, n.º 2, alíneas f) e j), do RGPD, de suspender ou de proibir essa transferência, sem limitar de forma alguma o exercício desse poder a circunstâncias excecionais.

115 Em qualquer caso, o poder de execução que o artigo 46.º, n.º 2, alínea c), do RGPD reconhece à Comissão para adotar cláusulas-tipo de proteção de dados não lhe confere a competência para limitar os poderes de que dispõem as autoridades de controlo ao abrigo do artigo 58.º, n.º 2, deste regulamento (v., por analogia, no que respeita ao artigo 25.º, n.º 6, e ao artigo 28.º da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.ºs 102 e 103). De resto, o considerando 5 da Decisão de Execução 2016/2297 confirma que a Decisão CPT «não impede uma [autoridade de controlo] de exercer as suas competências de supervisão dos fluxos de dados, incluindo o poder de suspender ou de proibir uma transferência de dados pessoais, se considerar que a transferência é efetuada em violação da legislação nacional ou da [União Europeia] em matéria de proteção de dados».

116 Todavia, importa precisar que os poderes da autoridade de controlo competente estão sujeitos ao pleno respeito da decisão pela qual a Comissão verifica, se for caso disso, em aplicação do artigo 45.º, n.º 1, primeiro período, do RGPD, que determinado país terceiro assegura um nível de proteção adequado. Com efeito, nessa hipótese, decorre do artigo 45.º, n.º 1, segundo período, deste regulamento, lido em conjugação com o seu considerando 103, que as transferências de dados pessoais para o país terceiro em causa podem ocorrer sem que seja necessário obter uma autorização específica.

117 Por força do artigo 288.º, quarto parágrafo, TFUE, uma decisão de adequação da Comissão possui, em todos os seus elementos, caráter obrigatório para todos os Estados-Membros destinatários e impõe-se, portanto, a todos os seus órgãos, na medida em que constate que o país terceiro em causa garante um nível adequado de proteção e que tenha por efeito autorizar essas transferências de dados (v., por analogia, no que respeita ao artigo 25.º, n.º 6, da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 51 e jurisprudência referida).

118 Assim, enquanto a decisão de adequação não for declarada inválida pelo Tribunal de Justiça, os Estados-Membros e os seus órgãos, entre os quais se encontram as respetivas 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 (Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 52 e jurisprudência referida) e, consequentemente, a suspender ou proibir transferências de dados pessoais para esse país terceiro.

119 Todavia, uma decisão de adequação da Comissão adotada nos termos do artigo 45.º, n.º 3, do RGPD não pode impedir as pessoas cujos dados pessoais tenham sido ou possam ser transferidos para um país terceiro de apresentarem, nos termos do artigo 77.º, n.º 1, do RGPD, à autoridade nacional de controlo competente, uma reclamação relativa à proteção dos seus direitos e liberdades no que diz respeito ao tratamento desses dados. De igual modo, 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 51.º, n.º 1, e pelo artigo 57.º, n.º 1, alínea a), do referido regulamento (v., por analogia, no que respeita ao artigo 25.º, n.º 6, e ao artigo 28.º da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 53).

120 Assim, mesmo perante uma decisão de adequação da Comissão, a autoridade nacional de controlo competente à qual uma pessoa tenha apresentado uma reclamação relativa à proteção dos seus direitos e liberdades no que diz respeito ao tratamento dos seus dados pessoais deve poder examinar, com total independência, se a transferência desses dados respeita as exigências estabelecidas pelo RGPD e, sendo caso disso, intentar uma ação nos órgãos jurisdicionais nacionais para que estes últimos, caso partilhem das dúvidas dessa autoridade quanto à validade da decisão de adequação, procedam a um reenvio prejudicial para efeitos da apreciação dessa validade (v., por analogia, no que respeita ao artigo 25.º, n.º 6, e ao artigo 28.º da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.ºs 57 e 65).

121 Atendendo às considerações anteriores, há que responder à oitava questão que o artigo 58.º, n.º 2, alíneas f) e j), do RGPD deve ser interpretado no sentido de que, a menos que exista uma decisão de adequação validamente adotada pela Comissão, a autoridade de controlo competente está obrigada a suspender ou a proibir uma transferência de dados para um país terceiro com base em cláusulas-tipo de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar, à luz de todas as circunstâncias específicas dessa transferência, que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União, em particular pelos artigos 45.º e 46.º do RGPD e pela Carta, não pode ser assegurada por outros meios, no caso de o responsável pelo tratamento ou o seu subcontratante estabelecidos na União não terem eles próprios suspendido ou posto termo à transferência.

Quanto à sétima e décima primeira questões

122 Com a sua sétima e décima primeira questões, que há que examinar em conjunto, o órgão jurisdicional de reenvio questiona o Tribunal de Justiça, em substância, sobre a validade da Decisão CPT à luz dos artigos 7.º, 8.º e 47.º da Carta.

123 Em particular, como resulta dos próprios termos da sétima questão e das explicações relativas a esta questão que figuram no pedido de decisão prejudicial, o órgão jurisdicional de reenvio interroga-se sobre se a Decisão CPT pode assegurar um nível de proteção adequado dos dados pessoais transferidos para países terceiros, na medida em que as cláusulas-tipo de proteção de dados nela previstas não vinculam as autoridades desses países terceiros.

124 O artigo 1.º da Decisão CPT dispõe que se considera que as cláusulas-tipo de proteção de dados que figuram no anexo desta decisão oferecem garantias adequadas de proteção da vida privada, bem como dos direitos e liberdades fundamentais das pessoas, em conformidade com as exigências do artigo 26.º, n.º 2, da Diretiva 95/46. Esta última disposição foi reproduzida, em substância, no artigo 46.º, n.º 1, e no artigo 46.º, n.º 2, alínea c), do RGPD.

125 Todavia, embora essas cláusulas sejam vinculativas para o responsável pelo tratamento estabelecido na União e para o destinatário da transferência de dados pessoais estabelecido num país terceiro, no caso de terem celebrado um contrato com referência a essas cláusulas, é pacífico que as referidas cláusulas não são suscetíveis de vincular as autoridades desse país terceiro, uma vez que estas últimas não são partes no contrato.

126 Por conseguinte, embora haja situações em que, em função do estado do direito e das práticas em vigor no país terceiro em causa, o destinatário dessa transferência esteja em condições de garantir a proteção dos dados necessária apenas com base nas cláusulas-tipo de proteção de dados, outras há em que as disposições constantes dessas cláusulas podem não constituir um meio suficiente para permitir assegurar, na prática, a proteção efetiva dos dados pessoais transferidos para o país terceiro em causa. É o que sucede, nomeadamente, quando o direito desse país terceiro permite às suas autoridades públicas ingerências nos direitos dos titulares dos dados relativos a esses dados.

127 Assim, coloca-se a questão de saber se uma decisão da Comissão relativa a cláusulas-tipo de proteção de dados, adotada com base no artigo 46.º, n.º 2, alínea c), do RGPD, é inválida, caso não existam nessa decisão garantias oponíveis às autoridades públicas dos países terceiros para os quais os dados pessoais são ou poderiam ser transferidos com base nessas cláusulas.

128 O artigo 46.º, n.º 1, do RGPD prevê que, na falta de uma decisão de adequação, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes. Segundo o artigo 46.º, n.º 2, alínea c), deste regulamento, essas garantias podem ser previstas por meio de cláusulas-tipo de proteção de dados adotadas pela Comissão. Ora, estas disposições não enunciam que todas as referidas garantias devem necessariamente ser previstas numa decisão da Comissão como a Decisão CPT.

129 A este respeito, importa salientar que uma decisão dessa natureza se distingue de uma decisão de adequação adotada ao abrigo do artigo 45.º, n.º 3, do RGPD, a qual, na sequência de um exame da regulamentação do país terceiro em causa, à luz, nomeadamente, da legislação pertinente em matéria de segurança nacional e de acesso das autoridades públicas aos dados pessoais, visa constatar com efeito vinculativo que um país terceiro, um território ou um ou mais setores específicos de um país terceiro garante um nível de proteção adequado e que, por conseguinte, o acesso das autoridades públicas do referido país terceiro a esses dados não obsta às transferências destes para esse mesmo país terceiro. Assim, tal decisão de adequação só pode ser adotada pela Comissão na condição de esta ter constatado que a legislação pertinente do país terceiro na matéria comporta efetivamente todas as garantias exigidas que permitam considerar que essa legislação assegura um nível de proteção adequado.

130 Em contrapartida, no que se refere a uma decisão da Comissão que adota cláusulas-tipo de proteção de dados, como a Decisão CPT, na medida em que tal decisão não visa um país terceiro, um território ou um ou mais setores específicos de um país terceiro, não se pode inferir do artigo 46.º, n.º 1, e do artigo 46.º, n.º 2, alínea c), do RGPD que a Comissão esteja obrigada, antes de adotar uma decisão dessa natureza, a proceder a uma avaliação do caráter adequado do nível de proteção assegurado pelos países terceiros para os quais os dados pessoais podem ser transferidos com base nessas cláusulas.

131 A este respeito, há que recordar que, nos termos do artigo 46.º, n.º 1, deste regulamento, não tendo sido tomada qualquer decisão de adequação pela Comissão, incumbe aos responsáveis pelo tratamento ou subcontratantes estabelecidos na União apresentar, nomeadamente, garantias adequadas. Os considerandos 108 e 114 do referido regulamento confirmam que, quando a Comissão não se tenha pronunciado sobre o caráter adequado do nível de proteção dos dados num país terceiro, o responsável pelo tratamento ou, se for caso disso, o seu subcontratante, «deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados» e que «[e]ssas medidas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes […] quer no território da União quer num país terceiro».

132 Uma vez que, como decorre do n.º 125 do presente acórdão, é inerente ao caráter contratual das cláusulas-tipo de proteção de dados que estas não podem vincular as autoridades públicas dos países terceiros, mas que o artigo 44.º, o artigo 46.º, n.º 1, e o artigo 46.º, n.º 2, alínea c), do RGPD, interpretados à luz dos artigos 7.º, 8.º e 47.º da Carta, exigem que o nível de proteção das pessoas singulares garantido por este regulamento não seja comprometido, pode revelar-se necessário complementar as garantias constantes dessas cláusulas-tipo de proteção de dados. A este respeito, o considerando 109 do referido regulamento enuncia que «[a] possibilidade de o responsável pelo tratamento […] [utilizar] cláusulas-tipo de proteção de dados adotadas pela Comissão […] não [o]

deverá impedir de […] [acrescentar] outras cláusulas ou garantias adicionais» e precisa, em particular, que estes «deverão ser encorajados a apresentar garantias suplementares […] que complementem as cláusulas-tipo de proteção [de dados]».

133 Afigura-se, assim, que as cláusulas-tipo de proteção de dados adotadas pela Comissão ao abrigo do artigo 46.º, n.º 2, alínea c), do mesmo regulamento visam unicamente fornecer aos responsáveis pelo tratamento ou aos seus subcontratantes estabelecidos na União garantias contratuais que se apliquem de maneira uniforme em todos os países terceiros e, como tal, independentemente do nível de proteção garantido em cada um deles. Na medida em que estas cláusulas-tipo de proteção de dados não podem, tendo em conta a sua natureza, fornecer garantias que vão além de uma obrigação contratual de assegurar que o nível de proteção exigido pelo direito da União seja respeitado, podem necessitar, em função da situação existente em determinado país terceiro, da adoção de medidas suplementares por parte do responsável pelo tratamento, a fim de assegurar o respeito desse nível de proteção.

134 A este respeito, como salientou o advogado-geral no n.º 126 das suas conclusões, o mecanismo contratual previsto no artigo 46.º, n.º 2, alínea c), do RGPD baseia-se na responsabilização do responsável pelo tratamento ou do seu subcontratante estabelecidos na União e, subsidiariamente, da autoridade de controlo competente. Por conseguinte, cabe, antes de mais, a esse responsável pelo tratamento ou ao seu subcontratante verificar, caso a caso e, se for caso disso, em colaboração com o destinatário da transferência, se o direito do país terceiro de destino assegura uma proteção adequada, à luz do direito da União, dos dados pessoais transferidos com base em cláusulas-tipo de proteção de dados, fornecendo, se necessário, garantias adicionais às oferecidas por essas cláusulas.

135 Caso não possam tomar medidas adicionais suficientes para garantir essa proteção, o responsável pelo tratamento ou o seu subcontratante estabelecidos na União ou, a título subsidiário, a autoridade de controlo competente são obrigados a suspender ou a pôr termo à transferência de dados pessoais para o país terceiro em causa. É o que acontece, nomeadamente, quando o direito desse país terceiro impõe ao destinatário de uma transferência de dados pessoais provenientes da União obrigações contrárias às referidas cláusulas e, portanto, suscetíveis de pôr em causa a garantia contratual de um nível de proteção adequado contra o acesso das autoridades públicas do referido país terceiro a esses dados.

136 Por conseguinte, o simples facto de as cláusulas-tipo de proteção de dados que figuram numa decisão da Comissão adotada em aplicação do artigo 46.º, n.º 2, alínea c), do RGPD, como as que figuram no anexo da Decisão CPT, não vincularem as autoridades dos países terceiros para os quais os dados pessoais são suscetíveis de ser transferidos não pode afetar a validade dessa decisão.

137 Esta validade depende, em contrapartida, da questão de saber se, em conformidade com a exigência resultante do artigo 46.º, n.º 1, e do artigo 46.º, n.º 2, alínea c), do RGPD, interpretados à luz dos artigos 7.º, 8.º e 47.º da Carta, tal decisão comporta mecanismos efetivos que permitam, na prática, garantir que o nível de proteção exigido pelo direito da União seja respeitado e que as transferências de dados pessoais, baseadas nessas cláusulas, sejam suspensas ou proibidas em caso de violação dessas cláusulas ou de impossibilidade de as honrar.

138 No que diz respeito às garantias contidas nas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT, decorre da cláusula 4, alíneas a) e b), da cláusula 5, alínea a), da cláusula 9, bem como da cláusula 11, n.º 1, desta decisão que o responsável pelo tratamento estabelecido na União, o destinatário da transferência de dados pessoais e o eventual subcontratante deste último se comprometem mutuamente a que o tratamento desses dados, incluindo a sua transferência, foi e continuará a ser efetuado em conformidade com a «legislação sobre proteção de dados aplicável», a saber, segundo a definição que figura no artigo 3.º, alínea f), da referida decisão, «a legislação que protege os direitos e as liberdades fundamentais das pessoas e, em especial, o seu direito à proteção

da vida privada no que diz respeito ao tratamento dos seus dados pessoais, aplicável a um responsável pelo tratamento dos dados no Estado-Membro em que o exportador de dados está estabelecido». Ora, as disposições do RGPD, lidas à luz da Carta, fazem parte desta legislação.

139 Além disso, o destinatário da transferência de dados pessoais estabelecido num país terceiro compromete-se, nos termos dessa cláusula 5, alínea a), a informar imediatamente o responsável pelo tratamento estabelecido na União do facto de eventualmente não poder cumprir as obrigações que lhe incumbem por força do contrato celebrado. Em particular, segundo a referida cláusula 5, alínea b), esse destinatário certifica que não tem qualquer razão para crer que a legislação que lhe é aplicável o impede de respeitar as obrigações que lhe incumbem por força do contrato e que se compromete a notificar imediatamente ao exportador de dados, logo que dela tiver conhecimento, qualquer alteração da legislação nacional que lhe é aplicável que possa ter um efeito adverso substancial nas garantias e obrigações conferidas pelas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT. Por outro lado, embora a cláusula 5, alínea d), i), permita ao destinatário da transferência de dados pessoais não comunicar ao responsável pelo tratamento estabelecido na União um pedido juridicamente vinculativo de divulgação dos dados pessoais por parte de uma autoridade competente para a aplicação da lei, em caso de legislação que o impeça, como uma proibição de caráter penal que vise preservar o segredo de um inquérito policial, ele está, no entanto, obrigado, em conformidade com a cláusula 5, alínea a), do anexo da Decisão CPT, a informar o responsável pelo tratamento do facto de não poder cumprir as cláusulas-tipo de proteção de dados.

140 Nos dois casos que prevê, essa cláusula 5, alíneas a) e b), confere ao responsável pelo tratamento estabelecido na União o direito de suspender a transferência de dados e/ou de rescindir o contrato. Tendo em conta as exigências resultantes do artigo 46.º, n.º 1, e n.º 2, alínea c), do RGPD, lido à luz dos artigos 7.º e 8.º da Carta, a suspensão da transferência de dados e/ou a rescisão do contrato têm caráter obrigatório para o responsável pelo tratamento, quando o destinatário da transferência não está, ou deixou de estar, em condições de respeitar as cláusulas-tipo de proteção de dados. Se assim não fosse, o responsável pelo tratamento violaria as exigências que lhe incumbem por força da cláusula 4, alínea a), do anexo da Decisão CPT, interpretada à luz das disposições do RGPD e da Carta.

141 Afigura-se, assim, que a cláusula 4, alínea a), e a cláusula 5, alíneas a) e b), desse anexo obrigam o responsável pelo tratamento estabelecido na União e o destinatário da transferência de dados pessoais a garantir que a legislação do país terceiro de destino permite ao referido destinatário respeitar as cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT, antes de proceder a uma transferência de dados pessoais para esse país terceiro. No que se refere a esta verificação, a nota de rodapé relativa à referida cláusula 5 expõe que os requisitos obrigatórios desta legislação que não excedam o necessário numa sociedade democrática para salvaguardar, nomeadamente, a segurança do Estado, a defesa e a segurança pública não são contrários ao disposto nas cláusulas-tipo de proteção de dados. Pelo contrário, como sublinhou o advogado-geral no n.º 131 das suas conclusões, a observância de uma obrigação imposta pelo direito do país terceiro de destino que exceda o necessário para esses efeitos deve ser considerada uma violação das referidas cláusulas. A apreciação, por esses operadores, da necessidade de tal obrigação deve, sendo caso disso, ter em conta a constatação do caráter adequado do nível de proteção garantido pelo país terceiro em causa, que figura na decisão de adequação da Comissão, adotada ao abrigo do artigo 45.º, n.º 3, do RGPD.

142 Daqui resulta que o responsável pelo tratamento estabelecido na União e o destinatário da transferência de dados pessoais são obrigados a verificar previamente o respeito, no país terceiro em causa, do nível de proteção exigido pelo direito da União. O destinatário dessa transferência tem a obrigação, se for caso disso, por força da mesma cláusula 5, alínea b), de informar o responsável pelo tratamento da sua eventual incapacidade de dar cumprimento a essas cláusulas, incumbindo então a este último suspender a transferência de dados e/ou rescindir o contrato.

143 Se o destinatário da transferência de dados pessoais para um país terceiro tiver comunicado ao responsável pelo tratamento, nos termos da cláusula 5, alínea b), do anexo da Decisão CPT, que a legislação do país terceiro em causa não lhe permite dar cumprimento às cláusulas-tipo de proteção de dados que figuram nesse anexo, decorre da cláusula 12 do referido anexo que os dados que já foram transferidos para esse país terceiro e as cópias devem, na sua totalidade, ser restituídos ou destruídos. Em qualquer caso, a cláusula 6 do mesmo anexo pune a violação dessas cláusulas-tipo, conferindo ao titular dos dados o direito de obter a reparação pelos danos sofridos.

144 Importa acrescentar que, segundo a cláusula 4, alínea f), do anexo da Decisão CPT, o responsável pelo tratamento estabelecido na União se compromete, no caso de categorias especiais de dados poderem ser transferidas para um país terceiro que não ofereça um nível de proteção adequado, a informar desse facto o titular dos dados, antes ou o mais depressa possível após a transferência. Essa informação pode dar a essa pessoa a possibilidade de exercer o direito de recurso que lhe é reconhecido pela cláusula 3, n.º 1, desse anexo contra o responsável pelo tratamento, para que este suspenda a transferência prevista, rescinda o contrato celebrado com o destinatário da transferência de dados pessoais ou, se for caso disso, peça a este último a restituição ou a destruição dos dados transferidos.

145 Por último, por força da cláusula 4, alínea g), do referido anexo, o responsável pelo tratamento estabelecido na União é obrigado, quando o destinatário da transferência de dados pessoais o notifica, em aplicação da cláusula 5, alínea b), desse anexo, de que a legislação que lhe é aplicável é objeto de uma alteração que pode ter um efeito adverso substancial nas garantias e obrigações conferidas pelas cláusulas-tipo de proteção de dados, a transmitir essa notificação à autoridade de controlo competente, se decidir, apesar da referida notificação, prosseguir a transferência ou levantar a sua suspensão. A transmissão de tal notificação a essa autoridade de controlo e o direito de esta proceder a auditorias junto do destinatário da transferência de dados pessoais em aplicação da cláusula 8, n.º 2, do mesmo anexo permitem à referida autoridade de controlo verificar se há que proceder à suspensão ou à proibição da transferência prevista, a fim de garantir um nível de proteção adequado.

146 Neste contexto, o artigo 4.º da Decisão CPT, lido à luz do considerando 5 da Decisão de Execução 2016/2297, confirma que a Decisão CPT não impede de modo algum a autoridade de controlo competente de suspender ou de proibir, se for caso disso, uma transferência de dados pessoais para um país terceiro com base nas cláusulas-tipo de proteção de dados que figuram no anexo dessa decisão. A este propósito, como decorre da resposta à oitava questão, a menos que exista uma decisão de adequação validamente adotada pela Comissão, a autoridade de controlo competente está obrigada, por força do artigo 58.º, n.º 2, alíneas f) e j), do RGPD, a suspender ou a proibir essa transferência, quando considere, à luz de todas as circunstâncias específicas dessa transferência, que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União não pode ser assegurada por outros meios, no caso de o responsável pelo tratamento ou o seu subcontratante estabelecidos na União não terem eles próprios suspendido ou posto termo à transferência.

147 Quanto à circunstância, salientada pelo Comissário, de as transferências de dados pessoais para esse país terceiro poderem eventualmente ser objeto de decisões divergentes das autoridades de controlo em diferentes Estados-Membros, importa acrescentar que, como decorre do artigo 55.º, n.º 1, e do artigo 57.º, n.º 1, alínea a), do RGPD, a missão de zelar pelo cumprimento deste regulamento é confiada, em princípio, a cada autoridade de controlo no território do Estado-Membro respetivo. Além disso, para evitar decisões divergentes, o artigo 64.º, n.º 2, do referido regulamento prevê a possibilidade de uma autoridade de controlo que considere que as transferências de dados para um país terceiro devem, de maneira geral, ser proibidas requerer um parecer do Comité Europeu para a Proteção de Dados (EDPB), podendo este, em aplicação do artigo 65.º, n.º 1, alínea c), do mesmo regulamento, adotar uma decisão vinculativa, nomeadamente quando uma autoridade de controlo não siga o parecer emitido.

148 Conclui-se que a Decisão CPT prevê mecanismos efetivos que permitem, na prática, assegurar que a transferência de dados pessoais para um país terceiro com base nas cláusulas-tipo de proteção de dados que figuram no anexo desta decisão seja suspensa ou proibida quando o destinatário da transferência não respeite as referidas cláusulas ou esteja impossibilitado de as respeitar.

149 Tendo em conta as considerações anteriores, há que responder à sétima e à décima primeira questão que o exame da Decisão CPT à luz dos artigos 7.º, 8.º e 47.º da Carta não revelou nenhum elemento suscetível de afetar a validade desta decisão.

Quanto à quarta, quinta, nona e décima questões

150 Com a sua nona questão, o órgão jurisdicional de reenvio pretende, em substância, saber se e em que medida uma autoridade de controlo de um Estado-Membro está vinculada pelas constatações que figuram na Decisão BPD segundo as quais os Estados Unidos garantem um nível de proteção adequado. Com a quarta, a quinta e a décima questão, esse órgão jurisdicional pergunta, em substância, se, tendo em conta as suas próprias constatações relativas ao direito dos Estados Unidos, a transferência de dados pessoais para esse país terceiro com base nas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT viola os direitos garantidos nos artigos 7.º, 8.º e 47.º da Carta e interroga o Tribunal de Justiça, em particular, sobre a questão de saber se a instituição do Mediador referido no anexo III da Decisão BPD é compatível com este artigo 47.º

151 A título preliminar, importa salientar que, embora a ação no processo principal intentada pelo Comissário ponha em causa a validade apenas da Decisão CPT, essa ação foi intentada no órgão jurisdicional de reenvio, antes da adoção da Decisão BPD. Na medida em que, com a quarta e a quinta questão, esse órgão jurisdicional interroga o Tribunal de Justiça, de maneira geral, sobre a proteção que deve ser garantida, por força dos artigos 7.º, 8.º e 47.º da Carta, no contexto dessa transferência, o exame do Tribunal de Justiça deve tomar em consideração as consequências resultantes da adoção da Decisão BPD, entretanto ocorrida. Isto é tanto mais assim que o referido órgão jurisdicional pergunta expressamente, com a sua décima questão, se a proteção exigida por este artigo 47.º é garantida por intermédio do Mediador mencionado nesta última decisão.

152 Além disso, decorre das indicações que figuram no pedido de decisão prejudicial que, no âmbito do processo principal, a Facebook Ireland alegou que a Decisão BPD produzia, para o Comissário, efeitos vinculativos no que respeita à constatação do caráter adequado do nível de proteção assegurado pelos Estados Unidos e, por conseguinte, quanto à licitude de uma transferência de dados pessoais para esse país terceiro com base nas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT.

153 Ora, como decorre do n.º 59 do presente acórdão, no seu Acórdão de 3 de outubro de 2017, anexado ao pedido de decisão prejudicial, o órgão jurisdicional de reenvio sublinhou que estava obrigado a ter em conta as alterações de direito ocorridas entre a interposição do recurso e a audiência realizada perante si. Assim, esse órgão jurisdicional parece estar obrigado a tomar em consideração, para dirimir o litígio no processo principal, a alteração de circunstâncias resultante da adoção da Decisão BPD bem como os eventuais efeitos vinculativos desta decisão.

154 Em particular, a existência dos efeitos vinculativos relacionados com a constatação, pela Decisão BPD, de um nível de proteção adequado nos Estados Unidos é relevante para fins de apreciação tanto das obrigações, recordadas nos n.ºs 141 e 142 do presente acórdão, que incumbem ao responsável pelo tratamento e ao destinatário de uma transferência de dados pessoais para um país terceiro efetuada com base nas cláusulas-tipo de proteção de dados que figuram no anexo da Decisão CPT como das obrigações que recaem, sendo caso disso, sobre a autoridade de controlo, de suspender ou de proibir essa transferência.

155 De facto, quanto aos efeitos vinculativos da Decisão BPD, o artigo 1.º, n.º 1, desta decisão dispõe que, para efeitos do artigo 45.º, n.º 1, do RGPD, «os Estados Unidos devem assegurar um nível de proteção adequado dos dados pessoais transferidos da União para organizações dos Estados Unidos ao abrigo do Escudo de Proteção da Privacidade [União Europeia]-EUA». Em conformidade com o artigo 1.º, n.º 3, daquela decisão, considera-se que os dados pessoais são transferidos ao abrigo deste escudo de proteção, sempre que sejam transferidos da União para organizações nos Estados Unidos que constem da lista das organizações aderentes ao referido escudo de proteção, mantida e disponibilizada ao público pelo Department of Commerce dos EUA, em conformidade com as secções I e III dos princípios estabelecidos no anexo II da mesma decisão.

156 Como resulta da jurisprudência recordada nos n.os 117 e 118 do presente acórdão, a Decisão BPD tem caráter vinculativo para as autoridades de controlo na medida em que constata que os Estados Unidos garantem um nível de proteção adequado e, portanto, tem por efeito autorizar transferências de dados pessoais efetuadas ao abrigo do Escudo de Proteção da Privacidade União Europeia-Estados Unidos. Por conseguinte, enquanto essa decisão não for declarada inválida pelo Tribunal de Justiça, a autoridade de controlo competente não pode suspender ou proibir uma transferência de dados pessoais para uma organização aderente a esse escudo de proteção, com o fundamento de que considera, contrariamente à apreciação feita pela Comissão naquela decisão, que a legislação dos Estados Unidos que regula o acesso aos dados pessoais transferidos ao abrigo do referido escudo de proteção e a utilização desses dados pelas autoridades públicas desse país terceiro, para efeitos de segurança nacional, de aplicação da lei ou de interesse público, não garante um nível de proteção adequado.

157 Não deixa de ser verdade que, em conformidade com a jurisprudência recordada nos n.os 119 e 120 do presente acórdão, quando uma pessoa lhe submete uma reclamação, a autoridade de controlo competente deve examinar, com toda a independência, se a transferência de dados pessoais em causa respeita as exigências impostas pelo RGPD e, caso considere procedentes as alegações apresentadas por essa pessoa para pôr em causa a validade de uma decisão de adequação, intentar uma ação nos órgãos jurisdicionais nacionais para que estes submetam ao Tribunal de Justiça um pedido de decisão prejudicial tendo por objeto a apreciação da validade dessa decisão.

158 Com efeito, uma reclamação apresentada ao abrigo do artigo 77.º, n.º 1, do RGPD, através da qual uma pessoa cujos dados pessoais tenham sido ou possam ser transferidos para um país terceiro alega que o direito e as práticas desse país não asseguram, não obstante o que a Comissão constatou numa decisão adotada nos termos do artigo 45.º, n.º 3, deste regulamento, um nível de proteção adequado, deve ser entendida no sentido de que tem por objeto, em substância, a compatibilidade dessa decisão com a proteção da vida privada bem como das liberdades e dos direitos fundamentais das pessoas (v., por analogia, no que respeita ao artigo 25.º, n.º 6, e ao artigo 28.º, n.º 4, da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 59).

159 No caso vertente, M. Schrems pediu, em substância, ao Comissário que proibisse ou suspendesse a transferência dos seus dados pessoais, pela Facebook Ireland, para a Facebook Inc., estabelecida nos Estados Unidos, com o fundamento de que este país terceiro não garantia um nível de proteção adequado. Uma vez que o Comissário, no termo de uma investigação sobre as alegações de M. Schrems, recorreu ao órgão jurisdicional de reenvio, este último parece, à luz das provas apresentadas e do debate contraditório realizado perante si, interrogar-se sobre a procedência das dúvidas de M. Schrems quanto ao caráter adequado do nível de proteção garantido no referido país terceiro, apesar daquilo que a Comissão, entretanto, constatou na Decisão BPD, o que levou esse órgão jurisdicional a submeter ao Tribunal de Justiça a quarta, quinta e décima questões prejudiciais.

160 Como salientou o advogado-geral no n.º 175 das suas conclusões, estas questões prejudiciais devem, assim, ser entendidas no sentido de que põem em causa, em substância, a conclusão da Comissão, que figura na Decisão BPD, segundo a qual os Estados Unidos garantem um nível adequado de proteção dos dados pessoais transferidos da União para esse país terceiro e, portanto, a validade desta decisão.

161 Atendendo às considerações enunciadas nos n.os 121 e 157 a 160 do presente acórdão e a fim de dar uma resposta completa ao órgão jurisdicional de reenvio, importa, pois, examinar se a Decisão BPD é conforme com as exigências que decorrem do RGPD, lido à luz da Carta (v., por analogia, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 67).

162 A adoção, pela Comissão, de uma decisão de adequação nos termos do artigo 45.º, n.º 3, do RGPD 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 (v., por analogia, no que respeita ao artigo 25.º, n.º 6, da Diretiva 95/46, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 96).

Quanto ao conteúdo da Decisão BPD

163 A Comissão constatou, no artigo 1.º, n.º 1, da Decisão BPD, que os Estados Unidos devem assegurar um nível de proteção adequado dos dados pessoais transferidos da União para organizações dos Estados Unidos ao abrigo do Escudo de Proteção da Privacidade União Europeia-Estados Unidos, sendo este constituído, nomeadamente, nos termos do artigo 1.º, n.º 2, dessa decisão, pelos princípios emitidos pelo Department of Commerce dos EUA em 7 de julho de 2016, tal como estabelecido no anexo II da referida decisão e nas declarações e compromissos oficiais constantes dos documentos enumerados nos anexos I e III a VII da mesma decisão.

164 Todavia, a Decisão BPD precisa igualmente, no ponto I.5 do seu anexo II, sob a epígrafe «Princípios do quadro do Escudo de Proteção da Privacidade [União Europeia]-EUA emitidos pelo Department of Commerce dos EUA», que a adesão a esses princípios pode ser limitada, nomeadamente, «para observar requisitos de segurança nacional, [de] interesse público ou [de] execução legal». Assim, à semelhança da Decisão 2000/520, esta decisão consagra o primado desses requisitos sobre os referidos princípios, primado por força do qual as organizações americanas autocertificadas que recebem dados pessoais da União estão obrigadas a afastar, sem limitação, os mesmos princípios, quando estes últimos entrem em conflito com os referidos requisitos e se revelem, portanto, incompatíveis com os mesmos (v., por analogia, no que respeita à Decisão 2000/520, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 86).

165 Atendendo ao seu caráter geral, a derrogação que figura no ponto I.5 do anexo II da Decisão BPD 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 (v., por analogia, no que respeita à Decisão 2000/520, Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 87). Mais especificamente, e como foi constatado na Decisão BPD, essas ingerências podem resultar do acesso aos dados pessoais transferidos da União para os Estados Unidos e da utilização desses dados pelas autoridades públicas americanas, no âmbito dos programas de vigilância PRISM e UPSTREAM, baseados na secção 702 da FISA e no E.O. 12333.

166 Neste contexto, a Comissão avaliou, nos considerandos 67 a 135 da Decisão BPD, as limitações e as garantias previstas na legislação dos Estados Unidos, nomeadamente na secção 702 da FISA, no E.O. 12333 e na PPD-28, no que se refere ao acesso e à utilização de dados pessoais, transferidos ao

abrigo do Escudo de Proteção da Privacidade União Europeia-Estados Unidos, pelas autoridades públicas americanas para efeitos de segurança nacional, de exercício de funções coercivas e outros fins de interesse público.

167 No final dessa avaliação, a Comissão constatou, no considerando 136 desta decisão, que «os EUA asseguram um nível de proteção adequado dos dados pessoais transferidos da União para organizações autocertificadas dos Estados Unidos», e entendeu, no considerando 140 da referida decisão, que, «com base nas informações disponíveis sobre a ordem jurídica dos EUA, […] qualquer ingerência por parte das autoridades públicas dos EUA nos direitos fundamentais das pessoas cujos dados são transferidos da União para os Estados Unidos da América ao abrigo do Escudo de Proteção da Privacidade para efeitos de segurança nacional, do exercício de funções coercivas ou outros efeitos de interesse público, e as subsequentes restrições impostas às organizações autocertificadas no que se refere à sua adesão aos princípios, serão limitadas ao que é estritamente necessário para a consecução do objetivo legítimo em questão, e que existe uma proteção jurídica eficaz contra tal ingerência».

Quanto à constatação relativa ao nível de proteção adequado

168 Atendendo aos elementos referidos pela Comissão na Decisão BPD e aos elementos dados como provados pelo órgão jurisdicional de reenvio no âmbito do processo principal, esse órgão jurisdicional tem dúvidas sobre a questão de saber se o direito dos Estados Unidos assegura, efetivamente, o nível de proteção adequado exigido pelo artigo 45.º do RGPD, lido à luz dos direitos fundamentais garantidos nos artigos 7.º, 8.º e 47.º da Carta. Em particular, o referido órgão jurisdicional considera que o direito desse país terceiro não prevê as limitações e as garantias necessárias relativamente às ingerências autorizadas pela sua regulamentação nacional e também não garante uma proteção jurisdicional efetiva contra tais ingerências. Quanto a este último aspeto, acrescenta que a instauração do Mediador para o Escudo de Proteção não pode, em seu entender, sanar essas lacunas, uma vez que este Mediador não pode ser equiparado a um tribunal, na aceção do artigo 47.º da Carta.

169 No que respeita, em primeiro lugar, aos artigos 7.º e 8.º da Carta, que fazem parte do nível de proteção exigido na União e cujo respeito deve ser constatado pela Comissão antes de adotar uma decisão de adequação ao abrigo do artigo 45.º, n.º 1, do RGPD, há que recordar que o artigo 7.º da Carta garante a todas as pessoas o direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. Quanto ao artigo 8.º, n.º 1, da Carta, reconhece expressamente a todas as pessoas o direito à proteção dos dados de caráter pessoal que lhes digam respeito.

170 Assim, o acesso a dados pessoais de uma pessoa singular, com vista à sua conservação ou à sua utilização, afeta o direito fundamental dessa pessoa ao respeito pela vida privada, garantido pelo artigo 7.º da Carta, na medida em que este direito diz respeito a todas as informações relativas a uma pessoa singular identificada ou identificável. Os ditos tratamentos de dados estão igualmente abrangidos pelo âmbito de aplicação do artigo 8.º da Carta, uma vez que constituem tratamentos de dados pessoais na aceção deste artigo e devem, por isso, necessariamente, respeitar as exigências de proteção de dados previstas neste artigo [v., neste sentido, Acórdãos de 9 de novembro de 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, n.ºs 49 e 52, e de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 29; e Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.ºs 122 e 123].

171 O Tribunal de Justiça já declarou que a comunicação de dados pessoais a um terceiro, como uma autoridade pública, constitui uma ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, seja qual for a utilização posterior das informações comunicadas. O mesmo se diga da conservação de dados pessoais e do acesso aos referidos dados com vista à sua utilização pelas autoridades públicas, independentemente da questão de saber se as informações relativas à vida privada em questão são ou não sensíveis, ou se os interessados sofreram ou não eventuais inconvenientes em razão dessa ingerência [v., neste sentido, Acórdãos de 20 de maio de 2003,

Österreichischer Rundfunk e o., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, n.os 74 e 75, e de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.os 33 a 36; e Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.os 124 e 126].

172 Todavia, os direitos consagrados nos artigos 7.º e 8.º da Carta não são prerrogativas absolutas, mas devem ser tomados em consideração de acordo com a sua função na sociedade [v., neste sentido, Acórdãos de 9 de novembro de 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, n.º 48 e jurisprudência referida, e de 17 de outubro de 2013, Schwarz, C-291/12, EU:C:2013:670, n.º 33 e jurisprudência referida; e Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 136].

173 A este respeito, importa igualmente salientar que, nos termos do artigo 8.º, n.º 2, da Carta, os dados pessoais devem, nomeadamente, ser tratados «para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei».

174 Além disso, em conformidade com o artigo 52.º, n.º 1, primeiro período, da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos por esta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Segundo o artigo 52.º, n.º 1, segundo período, da Carta, na observância do princípio da proporcionalidade, essas restrições a esses direitos e liberdades só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.

175 Importa acrescentar, quanto a este último aspeto, que a exigência segundo a qual qualquer restrição ao exercício de direitos fundamentais deve ser prevista por lei implica que a própria base legal que permite a ingerência nesses direitos deve definir o alcance da restrição ao exercício do direito em causa [Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.º 139 e jurisprudência referida].

176 Por último, para satisfazer o requisito da proporcionalidade segundo o qual as derrogações à proteção de dados pessoais e as suas restrições devem ocorrer na estrita medida do necessário, a regulamentação em causa que contenha a ingerência deve prever regras claras e precisas que regulem o alcance e a aplicação da medida em causa e imponham requisitos mínimos, de modo que as pessoas cujos dados foram transferidos disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. Essa regulamentação deve, em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida que preveja o tratamento desses dados, garantindo, assim, que a ingerência se limita ao estritamente necessário. A necessidade de dispor destas garantias é ainda mais importante quando os dados pessoais são sujeitos a um tratamento automatizado [v., neste sentido, Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.os 140 e 141 e jurisprudência referida].

177 Para este efeito, o artigo 45.º, n.º 2, alínea a), do RGPD precisa que, no âmbito da sua avaliação da adequação do nível de proteção garantido por um país terceiro, a Comissão tem em conta, nomeadamente, «os direitos dos titulares dos dados efetivos e oponíveis» cujos dados pessoais são transferidos.

178 No caso vertente, a constatação efetuada pela Comissão na Decisão BPD, segundo a qual os Estados Unidos garantem um nível de proteção substancialmente equivalente ao garantido na União pelo RGPD, lido à luz dos artigos 7.º e 8.º da Carta, foi posta em causa com o fundamento, nomeadamente, de que as ingerências que resultam dos programas de vigilância baseados na secção 702 da FISA e no E.O. 12333 não estão sujeitas a exigências que garantam, no cumprimento do princípio da proporcionalidade, um nível de proteção substancialmente equivalente ao garantido pelo artigo 52.º, n.º 1, segundo período, da Carta. Há, portanto, que examinar se esses programas de vigilância são

executados no respeito dessas exigências, sem que seja necessário verificar previamente o respeito, por esse país terceiro, de condições substancialmente equivalentes às previstas no artigo 52.º, n.º 1, primeiro período, da Carta.

179 A este propósito, no que se refere aos programas de vigilância baseados na secção 702 da FISA, a Comissão constatou, no considerando 109 da Decisão BPD, que, segundo a referida secção, «o FISC não autoriza medidas de vigilância individuais; em vez disso, autoriza programas de vigilância (tais como o PRISM e o UPSTREAM) com base em certificações anuais elaboradas pelo Attorney General e o Director of National Intelligence [(DNI)]». Como resulta desse considerando, o controlo exercido pelo FISC visa verificar se esses programas de vigilância correspondem ao objetivo de obter informações externas, mas não respeita à questão de saber «se as pessoas são adequadamente visadas para efeitos de obtenção de informações externas».

180 Assim, a secção 702 da FISA não revela de forma alguma a existência de limitações à habilitação que essa disposição comporta com vista à execução dos programas de vigilância para efeitos de obtenção de informações externas nem a existência de garantias para as pessoas não americanas potencialmente visadas por esses programas. Nestas condições, e como salientou o advogado-geral, em substância, nos n.os 291, 292 e 297 das suas conclusões, esta disposição não é suscetível de assegurar um nível de proteção substancialmente equivalente ao garantido pela Carta, conforme interpretada pela jurisprudência recordada nos n.os 175 e 176 do presente acórdão, segundo a qual a própria base jurídica que permite ingerências nos direitos fundamentais deve, para satisfazer o princípio da proporcionalidade, definir o alcance da restrição ao exercício do direito em causa e prever regras claras e precisas que regulem o alcance e a aplicação da medida e imponham requisitos mínimos.

181 Segundo as constatações que figuram na Decisão BPD, os programas de vigilância baseados na secção 702 da FISA devem, é certo, ser executados em observância dos requisitos que resultam da PPD-28. Todavia, embora a Comissão tenha sublinhado, nos considerandos 69 e 77 da Decisão BPD, que tais requisitos têm caráter vinculativo para os serviços de informações americanos, o Governo americano admitiu, em resposta a uma questão do Tribunal de Justiça, que a PPD-28 não confere aos titulares dos dados direitos oponíveis às autoridades americanas nos tribunais. Por conseguinte, a PPD-28 não é suscetível de garantir um nível de proteção substancialmente equivalente ao que resulta da Carta, contrariamente ao que exige o artigo 45.º, n.º 2, alínea a), do RGPD, segundo o qual a constatação desse nível depende, nomeadamente, da existência de direitos efetivos e oponíveis de que beneficiam os titulares dos dados cujos dados foram transferidos para o país terceiro em causa.

182 No que se refere aos programas de vigilância baseados no E.O. 12333, decorre dos autos de que dispõe o Tribunal de Justiça que esse decreto também não confere direitos oponíveis às autoridades americanas nos tribunais.

183 Importa acrescentar que a PPD-28, que deve ser respeitada no âmbito da aplicação dos programas referidos nos dois números anteriores, permite proceder a uma «recolha em larga escala […] de um volume relativamente elevado de informações ou dados de origem eletromagnética em circunstâncias em que o setor das informações não pode utilizar um identificador associado a um objetivo específico […] para centrar a recolha», tal como é precisado numa carta de 21 de junho de 2016 do Gabinete do Diretor dos Serviços Nacionais de Informações (Office of the Director of National Intelligence) para o Department of Commerce americano e para a International Trade Administration, que figura no anexo VI da Decisão BPD. Ora, esta possibilidade, que, no âmbito dos programas de vigilância baseados no E.O. 12333, permite aceder a dados em trânsito para os Estados Unidos, sem que esse acesso seja objeto de qualquer supervisão judicial, não enquadra, em todo o caso, de forma suficientemente clara e precisa o alcance dessa recolha em larga escala de dados pessoais.

184 Por conseguinte, nem a secção 702 da FISA nem o E.O. 12333, lidos em conjugação com a PPD-28, correspondem aos requisitos mínimos inerentes, no direito da União, ao princípio da proporcionalidade, pelo que não se pode considerar que os programas de vigilância baseados nessas disposições se limitem ao estritamente necessário.

185 Nestas condições, as limitações da proteção de dados pessoais que decorrem da regulamentação interna dos Estados Unidos relativa ao acesso e à utilização, pelas autoridades públicas americanas, desses dados transferidos da União para os Estados Unidos, e que a Comissão avaliou na Decisão BPD, não estão enquadradas de forma a satisfazer os requisitos substancialmente equivalentes aos exigidos, no direito da União, no artigo 52.º, n.º 1, segundo período, da Carta.

186 No que se refere, em segundo lugar, ao artigo 47.º da Carta, que faz igualmente parte do nível de proteção exigido na União e cuja observância deve ser constatada pela Comissão antes de adotar uma decisão de adequação ao abrigo do artigo 45.º, n.º 1, do RGPD, importa recordar que o primeiro parágrafo deste artigo 47.º exige que toda a pessoa cujos direitos e liberdades garantidos pelo direito da União tenham sido violados tem direito a uma ação perante um tribunal nos termos previstos nesse artigo. Nos termos do segundo parágrafo deste artigo, toda a pessoa tem direito a que a sua causa seja julgada por um tribunal independente e imparcial.

187 Segundo jurisprudência constante, 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. Assim, uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a medidas jurídicas corretivas eficazes 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 (Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 95 e jurisprudência referida).

188 Para este efeito, o artigo 45.º, n.º 2, alínea a), do RGPD exige que, no âmbito da sua avaliação da adequação do nível de proteção garantido por um país terceiro, a Comissão tenha em conta, nomeadamente, as «vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência». O considerando 104 do RGPD sublinha, a este respeito, que o país terceiro «deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer regras de cooperação com as autoridades de proteção de dados dos Estados-Membros» e precisa que este deve «ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial».

189 A existência de tais vias efetivas de recurso no país terceiro em causa reveste particular importância no contexto de uma transferência de dados pessoais para esse país terceiro, na medida em que, como decorre do considerando 116 do RGPD, os titulares dos dados podem confrontar-se com a insuficiência dos poderes e dos meios das autoridades administrativas e judiciais dos Estados-Membros para dar seguimento útil às suas reclamações fundadas num tratamento alegadamente ilegal, nesse país terceiro, dos seus dados assim transferidos, o que é suscetível de os obrigar a dirigirem-se às autoridades e aos órgãos jurisdicionais nacionais desse país terceiro.

190 No caso vertente, a constatação feita pela Comissão, na Decisão BPD, de que os Estados Unidos asseguram um nível de proteção substancialmente equivalente ao garantido no artigo 47.º da Carta foi posta em causa pelo facto, nomeadamente, de a instauração do Mediador para o Escudo de Proteção da Privacidade não poder colmatar as lacunas verificadas pela própria Comissão no que respeita à proteção jurisdicional das pessoas cujos dados pessoais são transferidos para esse país terceiro.

191 A este respeito, a Comissão salientou, no considerando 115 da Decisão BPD, que, embora «as pessoas, incluindo os titulares de dados da [União], disponham de várias vias de recurso se tiverem sido objeto de vigilância (eletrónica) ilegal para efeitos de segurança nacional, é igualmente evidente que pelo menos algumas bases jurídicas que os serviços de informações dos EUA podem utilizar (por exemplo

E.O. 12333) não são abrangidas». Assim, no que se refere à E.O. 12333, a Comissão pôs a tónica, no referido considerando 115, na inexistência de qualquer via de recurso. Ora, segundo a jurisprudência recordada no n.º 187 do presente acórdão, essa lacuna na proteção jurisdicional relativamente às ingerências relacionadas com os programas de informações baseados nesse decreto presidencial obsta a que se conclua, como fez a Comissão na Decisão BPD, que o direito dos Estados Unidos assegura um nível de proteção substancialmente equivalente ao garantido no artigo 47.º da Carta.

192 Por outro lado, no que respeita tanto aos programas de vigilância baseados na secção 702 da FISA como aos baseados no E.O. 12333, foi salientado nos n.os 181 e 182 do presente acórdão que nem a PPD-28 nem o E.O. 12333 conferem aos titulares dos dados direitos oponíveis às autoridades americanas nos tribunais, pelo que esses titulares não dispõem de um direito a uma ação.

193 Todavia, nos considerandos 115 e 116 da Decisão BPD, a Comissão constatou que, devido à existência do mecanismo de mediação instituído pelas autoridades americanas, conforme descrito na carta dirigida em 7 de julho de 2016 pelo secretário de Estado americano à comissária europeia responsável pela Justiça, Consumidores e Igualdade de Género, que figura no anexo III dessa decisão, e à natureza da missão confiada ao Mediador, neste caso, um «Senior Coordinator for International Information Technology Diplomacy» [coordenador principal da diplomacia internacional em matéria de tecnologia da informação], se pode considerar que os Estados Unidos asseguram um nível de proteção substancialmente equivalente ao garantido no artigo 47.º da Carta.

194 O exame da questão de saber se o mecanismo de mediação previsto na Decisão BPD é efetivamente suscetível de atenuar as limitações do direito a uma proteção jurisdicional constatadas pela Comissão deve, em conformidade com os requisitos que decorrem do artigo 47.º da Carta e da jurisprudência recordada no n.º 187 do presente acórdão, partir do princípio de que os particulares devem dispor da possibilidade de recorrer a medidas jurídicas corretivas eficazes num tribunal independente e imparcial, para ter acesso a dados pessoais que lhes digam respeito ou para obter a retificação ou a supressão desses dados.

195 Ora, na carta evocada no n.º 193 do presente acórdão, o Mediador para o Escudo de Proteção da Privacidade, embora descrito como sendo «independente do setor das informações», foi apresentado como «[respondendo] diretamente perante o [s]ecretário de Estado, que assegurará que este desempenhe as suas funções de forma objetiva e isenta de influências indevidas que possa[m] afetar a resposta a fornecer». Por outro lado, além do facto de, como a Comissão constatou no considerando 116 dessa decisão, o Mediador ser nomeado pelo secretário de Estado e fazer parte integrante do Departamento de Estado dos Estados Unidos, não existe, na referida decisão, como salientou o advogado-geral no n.º 337 das suas conclusões, nenhuma indicação de que a destituição do Mediador ou a anulação da sua nomeação sejam acompanhadas de garantias especiais, o que pode pôr em causa a independência do Mediador relativamente ao poder executivo (v., neste sentido, Acórdão de 21 de janeiro de 2020, Banco de Santander, C-274/14, EU:C:2020:17, n.os 60 e 63 e jurisprudência referida).

196 Do mesmo modo, como sublinhou o advogado-geral no n.º 338 das suas conclusões, embora o considerando 120 da Decisão BPD refira um compromisso do Governo americano em como os serviços de informação em questão são obrigados a corrigir qualquer violação das normas aplicáveis detetada pelo Mediador para o Escudo de Proteção da Privacidade, a referida decisão não contém nenhuma indicação de que esse Mediador esteja habilitado a adotar decisões vinculativas para esses serviços e também não menciona garantias legais que acompanhem esse compromisso e que possam ser invocadas pelos titulares dos dados.

197 Por conseguinte, o mecanismo de mediação previsto na Decisão BPD não apresenta nenhuma via de recurso num órgão, que ofereça às pessoas cujos dados são transferidos para os Estados Unidos garantias substancialmente equivalentes às exigidas no artigo 47.º da Carta.

198 Consequentemente, ao declarar, no artigo 1.º, n.º 1, da Decisão BPD, que os Estados Unidos asseguram um nível de proteção adequado dos dados pessoais transferidos da União para organizações estabelecidas nesse país terceiro ao abrigo do Escudo de Proteção da Privacidade União Europeia-Estados Unidos, a Comissão violou os requisitos resultantes do artigo 45.º, n.º 1, do RGPD, lido à luz dos artigos 7.º, 8.º e 47.º da Carta.

199 Conclui-se que o artigo 1.º da Decisão BPD é incompatível com o artigo 45.º, n.º 1, do RGPD, lido à luz dos artigos 7.º, 8.º e 47.º da Carta, e que, por esta razão, é inválido.

200 Uma vez que o artigo 1.º da Decisão BPD é indissociável dos artigos 2.º a 6.º e dos seus anexos, a sua invalidade tem por efeito afetar a validade desta decisão no seu todo.

201 Atendendo às considerações anteriores, há que concluir que a Decisão BPD é inválida.

202 Quanto à questão de saber se se devem manter os efeitos desta decisão a fim de evitar a criação de um vazio jurídico (v., neste sentido, Acórdão de 28 de abril de 2016, Borealis Polyolefine e o., C-191/14, C-192/14, C-295/14, C-389/14 e C-391/14 a C-393/14, EU:C:2016:311, n.º 106), observe-se que, em qualquer caso, atendendo ao artigo 49.º do RGPD, a anulação de uma decisão de adequação como a Decisão BPD não é suscetível de criar tal vazio jurídico. Com efeito, este artigo estabelece, de forma precisa, as condições em que as transferências de dados pessoais para países terceiros podem ocorrer na falta de uma decisão de adequação ao abrigo do artigo 45.º, n.º 3, do referido regulamento ou de garantias adequadas nos termos do artigo 46.º do mesmo regulamento.

Quanto às despesas

203 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 Secção) declara:

1) **O artigo 2.º, n.os 1 e 2, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), deve ser interpretado no sentido de que está abrangida pelo âmbito de aplicação deste regulamento uma transferência de dados pessoais efetuada para fins comerciais por um operador económico estabelecido num Estado-Membro para outro operador económico estabelecido num país terceiro, não obstante o facto de, no decurso ou na sequência dessa transferência, esses dados serem suscetíveis de ser tratados pelas autoridades do país terceiro em causa para efeitos de segurança pública, de defesa e de segurança do Estado.**

2) **O artigo 46.º, n.º 1, e o artigo 46.º, n.º 2, alínea c), do Regulamento 2016/679 devem ser interpretados no sentido de que as garantias adequadas, os direitos oponíveis e as medidas jurídicas corretivas eficazes, exigidos por estas disposições, devem assegurar que os direitos das pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas-tipo de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União Europeia por este regulamento, lido à luz da Carta dos Direitos Fundamentais da União Europeia. Para este efeito, a avaliação do nível de proteção assegurado no contexto dessa transferência deve, nomeadamente, ter em consideração tanto as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União Europeia e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das**

autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro, nomeadamente os enunciados no artigo 45.º, n.º 2, do referido regulamento.

3) **O artigo 58.º, n.º 2, alíneas f) e j), do Regulamento 2016/679 deve ser interpretado no sentido de que, a menos que exista uma decisão de adequação validamente adotada pela Comissão Europeia, a autoridade de controlo competente está obrigada a suspender ou a proibir uma transferência de dados para um país terceiro com base em cláusulas-tipo de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar, à luz de todas as circunstâncias específicas dessa transferência, que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União, em particular pelos artigos 45.º e 46.º deste regulamento e pela Carta dos Direitos Fundamentais, não pode ser assegurada por outros meios, no caso de o responsável pelo tratamento ou o seu subcontratante estabelecidos na União não terem eles próprios suspendido ou posto termo à transferência.**

4) **O exame da Decisão 2010/87/UE da Comissão, de 5 de fevereiro de 2010, relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, conforme alterada pela Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de dezembro de 2016, à luz dos artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais não revelou nenhum elemento suscetível de afetar a validade desta decisão.**

5) **A Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, é inválida.**

Assinaturas