COMISSÃO
EUROPEIA

Bruxelas, 6.11.2015
COM(2015) 566 final

# COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

## sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems)

**COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO**

**sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems)**

# 1. INTRODUÇÃO: A ANULAÇÃO DA DECISÃO «PORTO SEGURO»

O acórdão do Tribunal de Justiça da União Europeia (a seguir designado «Tribunal de Justiça» ou «Tribunal»), de 6 de outubro de 2015, no processo C-362/14 (Schrems)[1], reafirma a importância do direito fundamental à proteção dos dados pessoais, consagrado na Carta dos Direitos Fundamentais da UE, mesmo quando esses dados são transferidos para fora da União.

As transferências de dados pessoais são um elemento essencial das relações transatlânticas. A UE é o parceiro comercial mais importante dos Estados Unidos, tal como os Estados Unidos são o parceiro comercial mais importante da UE, constituindo as transferências de dados, cada vez mais, uma parte integrante das suas trocas comerciais.

A fim de facilitar esses fluxos de dados, assegurando simultaneamente um elevado nível de proteção dos dados pessoais, a Comissão reconheceu a adequação do enquadramento de «porto seguro» através da adoção da Decisão 2000/520/CE da Comissão, de 20 de julho de 2000 (a seguir designada «Decisão Porto Seguro»). Nesta decisão, baseada no artigo 25.º, n.º 6, da Diretiva 95/46/CE[2], a Comissão tinha reconhecido os princípios de «porto seguro» e as questões mais frequentes (FAQ) que os acompanhavam, emitidos pelo Departamento do Comércio (Department of Commerce) dos Estados Unidos, como proporcionando proteção adequada às transferências de dados pessoais da UE[3]. Em seu resultado, os dados pessoais podiam ser livremente transferidos dos Estados-Membros da UE para empresas nos Estados Unidos signatárias dos princípios, não obstante a ausência de uma lei geral de proteção de dados nos Estados Unidos. O funcionamento de acordos de tipo «porto seguro» baseava-se em compromissos e na auto certificação das empresas participantes. Embora a adesão aos princípios de «porto seguro» e às FAQ seja voluntária, tais regras são vinculativas na aceção da legislação dos EUA para as entidades que as tenham subscrito e o seu respeito pode ser imposto pela Comissão Federal do Comércio (Federal Trade Commission) dos EUA[4].

---

1 Acórdão de 6 de outubro de 2015 no processo C-362/14, Maximilian Schrems/Data Protection Commissioner, EU:C:2015:650 (a seguir designado também como «acórdão» ou «acórdão Schrems»).

2 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, JO L 281 de 23.11.95. p. 31 (a seguir designada «Diretiva 95/46/CE» ou «Diretiva»).

3 Para efeitos da presente comunicação, o termo «UE» abrange igualmente o EEE. Por conseguinte, as referências a «Estados-Membros» entender-se-ão como abrangendo também os Estados membros do EEE.

4 Para obter uma panorâmica mais aprofundada do acordo «porto seguro», consultar a Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE, COM/2013/847 final.

No seu acórdão de 6 de outubro de 2015, o Tribunal declarou a nulidade da Decisão Porto Seguro. É neste contexto que a presente comunicação visa fornecer uma panorâmica dos instrumentos alternativos para as transferências transatlânticas de dados ao abrigo da Diretiva 95/46/CE na falta de uma decisão de adequação. Descreve igualmente de forma resumida as consequências do acórdão relativamente a outras decisões de adequação da Comissão. No acórdão, o Tribunal clarificou que uma decisão de adequação nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE, está subordinada à determinação, por parte da Comissão, de que no país terceiro em questão existe um nível de proteção de dados pessoais que, embora não necessariamente idêntico, seja «essencialmente equivalente» ao que é garantido na UE por força da diretiva, interpretada à luz da Carta dos Direitos Fundamentais. No que se refere especificamente à Decisão Porto Seguro, o Tribunal defendeu que não continha provas suficientes por parte da Comissão das restrições de acesso das autoridades públicas dos EUA aos dados transferidos ao abrigo dessa decisão e sobre a existência de uma proteção jurídica efetiva contra tais interferências. Em particular, o Tribunal esclareceu que a legislação que permita às autoridades públicas o acesso generalizado ao conteúdo das comunicações eletrónicas deve ser considerada como comprometendo a essência do direito fundamental ao respeito pela vida privada. Além disso, o Tribunal confirmou que, ainda que exista uma decisão de adequação nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE, as autoridades de proteção de dados (APD) dos Estados-Membros continuam a deter poderes e a estar obrigadas a examinar, com total independência, se as transferências de dados para um país terceiro cumprem os requisitos previstos pela Diretiva 95/46/CE interpretada à luz dos artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais. Contudo, o Tribunal também afirmou que unicamente o Tribunal de Justiça pode declarar um ato da UE - designadamente uma decisão de adequação da Comissão - inválido.

O acórdão do Tribunal tem por base a Comunicação da Comissão de 2013 sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE[5], na qual a Comissão identificou uma série de lacunas e propôs 13 recomendações. Com base nessas recomendações, a Comissão manteve conversações com as autoridades dos Estados Unidos, desde janeiro de 2014, com o objetivo de estabelecer um acordo transatlântico renovado e reforçado para o intercâmbio de dados.

Na sequência do acórdão, a Comissão mantém o seu empenhamento em estabelecer um quadro renovado e sólido para as transferências transatlânticas de dados pessoais. A este respeito, reiniciou e intensificou de imediato as conversações com o governo americano, de forma a garantir que qualquer novo acordo para a transferência transatlântica de dados pessoais cumpra plenamente as normas definidas pelo Tribunal. Tal quadro deve, portanto, prever limitações suficientes, garantias e mecanismos de controlo jurisdicional criados para assegurar a proteção permanente dos dados pessoais dos cidadãos da UE, mesmo no que se

[5] Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE, COM(2013) 847 final de 27.11.2013. Ver também a Comunicação da Comissão ao Parlamento Europeu e ao Conselho, intitulada «Restabelecer a confiança nos fluxos de dados entre a UE e os EUA», COM(2013) 846 final de 27.11.2013, e o Memorando relacionado, intitulado «Restabelecer a confiança nos fluxos de dados entre a UE e os EUA – questões mais frequentes», MEMO/13/1059, 27.11.2013.

refere ao eventual acesso por parte das autoridades públicas para fins repressivos e de segurança nacional. Entretanto, a indústria expressou a sua preocupação no que se refere à possibilidade de continuar a transferir dados[6]. Existe, por isso, a necessidade de esclarecer em que condições essas transferências podem continuar. Tal levou o Grupo de Trabalho do artigo 29.º, o órgão consultivo independente que reúne representantes de todas as autoridades de proteção de dados dos Estados-Membros, bem como a Autoridade Europeia para a Proteção de Dados, a emitir, a 16 de outubro, uma declaração[7] relativa às primeiras conclusões a retirar do acórdão. Entre outros pontos, esta declaração continha as seguintes orientações para a transferência de dados:

– As transferências de dados deixam de se poder basear na Decisão Porto Seguro invalidada da Comissão;

– As cláusulas-tipo de proteção de dados (a seguir também «SCC») e as regras vinculativas para empresas (a seguir também «BCR») podem, entretanto, ser utilizadas como base para as transferências de dados, embora o Grupo de Trabalho do artigo 29.º tenha declarado igualmente que continuará a analisar o impacto do acórdão sobre estes instrumentos alternativos.

A declaração convidava ainda os Estados-Membros e as instituições da UE a dialogarem com as autoridades americanas com vista a encontrar soluções técnicas e jurídicas para as transferências de dados; as negociações para um novo acordo «porto seguro» poderiam, na opinião do Grupo de Trabalho do artigo 29.º, ser parte dessa solução.

O Grupo de Trabalho do artigo 29.º anunciou que, se até final de janeiro de 2016 não for encontrada nenhuma solução adequada junto das autoridades americanas, e em função da avaliação dos instrumentos alternativos para as transferências de dados, as autoridades de proteção de dados tomarão todas as medidas necessárias e apropriadas, incluindo uma ação de execução coordenada.

Por fim, o Grupo de Trabalho do artigo 29.º salientou a responsabilidade partilhada das autoridades de proteção de dados, das instituições da UE, dos Estados-Membros e das empresas para encontrarem soluções sustentáveis no sentido de dar execução ao acórdão do

---

6 Representantes de associações da indústria manifestaram as suas preocupações, nomeadamente, numa reunião organizada pouco depois do acórdão Schrems pelo Vice-Presidente Ansip e os Comissários Jourová e Oettinger, a 14 de outubro. Ver *Daily News* de 14.10.2015 (MEX/15/5840). Ver também: *Open letter on the implementation of the CJEU Judgement on Case C-362/14 Maximillian Schrems v Data Protection Commissioner* (carta aberta sobre a execução do acórdão do Tribunal de Justiça da União Europeia no processo C-362/14 entre Maximillian Schrems/Data Protection Commissioner), de 13 de outubro de 2015, dirigida ao Presidente da Comissão, Jean-Claude Juncker, e assinada por várias associações e empresas da indústria da UE e dos EUA: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353

7 Declaração do Grupo de Trabalho do artigo 29.º, disponível na Internet em: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

Tribunal. Em particular, o Grupo de Trabalho exortou as empresas a ponderarem a introdução de soluções técnicas e jurídicas para mitigar eventuais riscos que possam correr quando transferem dados.

A presente comunicação não prejudica as competências e os deveres das autoridades de proteção de dados para examinarem a legitimidade dessas transferências com total independência[8]. Não estabelece qualquer regra vinculativa e respeita plenamente as competências dos tribunais nacionais para interpretarem a lei aplicável e, quando necessário, consultarem o Tribunal de Justiça para obter uma decisão a título prejudicial. A presente comunicação não pode, igualmente, constituir uma base para a reivindicação de qualquer direito individual ou coletivo ou ação de reparação.

## 2. BASES ALTERNATIVAS PARA AS TRANSFERÊNCIAS DE DADOS PESSOAIS PARA OS EUA

As regras em matéria de transferências internacionais de dados, estabelecidas na Diretiva 95/46/CE, baseiam-se numa clara distinção entre, por um lado, as transferências para países terceiros que asseguram um nível de proteção adequado (artigo 25.º da Diretiva) e, por outro, as transferências para países terceiros que se concluiu que não asseguram um nível de proteção adequado (artigo 26.º da Diretiva).

O acórdão Schrems aborda as condições ao abrigo das quais, na aceção do artigo 25.º, n.º 6, da Diretiva 95/46/CE, a Comissão pode determinar que um país terceiro assegura um nível de proteção adequado.

Se for considerado que o país terceiro para o qual os dados pessoais devem ser exportados a partir da UE não assegura esse nível de proteção adequado, o artigo 26.º da Diretiva 95/46/CE prevê uma série de motivos alternativos com base nos quais as transferências poderão, não obstante, ser realizadas. Em particular, tais transferências podem ser realizadas desde que a entidade responsável pela determinação dos fins e meios do tratamento dos dados pessoais (o «responsável pelo tratamento»):

– apresente garantias suficientes, na aceção do artigo 26.º, n.º 2, da Diretiva 95/46/CE, de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, bem como do exercício dos respetivos direitos. Essas garantias podem, nomeadamente, ser fornecidas por meio de cláusulas contratuais que vinculem o exportador e o importador dos dados (ver secções 2.1 e 2.2 infra). Estas incluem cláusulas contratuais-tipo emitidas pela Comissão e, no que se refere às transferências entre as diferentes entidades de um grupo empresarial multinacional, as regras vinculativas para as empresas autorizadas pelas autoridades de proteção de dados; ou

[8] Ver o artigo 8.º, n.º 3, da Carta dos Direitos Fundamentais e o artigo 16.º, n.º 2, do Tratado sobre o Funcionamento da União Europeia. Esta independência foi também sublinhada pelo Tribunal no seu acórdão Schrems.

– se baseie numa das derrogações expressamente indicadas nas alíneas a) a f) do artigo 26.º, n.º 1, da Diretiva 95/46/CE (ver secção 2.3 infra).

Em comparação com as decisões de adequação que resultam da avaliação global do sistema de um determinado país terceiro e podem, em princípio, cobrir todas as transferências para esse sistema, estas bases alternativas para transferências têm um âmbito mais limitado (uma vez que se aplicam apenas a fluxos de dados específicos) e, simultaneamente, uma cobertura mais ampla (pois não estão necessariamente confinadas a um país específico). Aplicam-se a fluxos de dados realizados por entidades particulares que decidiram fazer uso de uma das possibilidades previstas no artigo 26.º da Diretiva 95/46/CE. Além disso, ao basearem desta forma as suas transferências, e como não podem invocar uma decisão de adequação do país terceiro adotada pela Comissão, os exportadores e importadores de dados têm a responsabilidade de assegurar que as transferências cumprem os requisitos da Diretiva.

## 2.1. Soluções contratuais

Conforme sublinhado pelo Grupo de Trabalho do artigo 29.º, a fim de proporcionar garantias suficientes para efeitos do artigo 26.º, n.º 2, da Diretiva 95/46/CE, as cláusulas contratuais «devem compensar, de forma satisfatória, a ausência de um nível geral de proteção adequada, incluindo os elementos essenciais de proteção que faltam numa determinada situação em particular»[9]. Com o objetivo de facilitar o uso de tais instrumentos nas transferências internacionais, a Comissão aprovou, em conformidade com o artigo 26.º, n.º 4, da Diretiva, quatro conjuntos de cláusulas contratuais-tipo considerados como respeitando os requisitos do artigo 26.º, n.º 2, da Diretiva. Dois conjuntos de cláusulas-tipo estão relacionados com as transferências entre responsáveis pelo tratamento de dados[10], enquanto os outros dois conjuntos dizem respeito às transferências entre um responsável pelo tratamento de dados e um subcontratante atuando sob instruções daquele[11]. Cada um destes conjuntos de cláusulas-tipo estabelece as obrigações respetivas dos exportadores e dos importadores de dados. Estas incluem obrigações relativas, designadamente, às medidas de segurança, à informação do titular dos dados em caso de transferência de dados sensíveis, à notificação ao exportador de dados dos pedidos de acesso pelas autoridades competentes pela aplicação da lei dos países terceiros ou de qualquer acesso acidental ou não autorizado, bem como aos direitos dos titulares dos dados em matéria de acesso, retificação e supressão dos seus dados

9 Ver Grupo de Trabalho do artigo 29.º, «Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva relativa à proteção de dados» (WP 12), de 24 de julho de 1998, p. 16.

10 Decisão 2001/497/CE da Comissão, de 15 de junho de 2001, sobre cláusulas-tipo de proteção de dados para a transferência de dados pessoais para países terceiros ao abrigo da Diretiva 95/46/CE, JO L 181, 4.7.2001, p. 19, e Decisão 2004/915/CE da Comissão, de 27 de dezembro de 2004, que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas-tipo de proteção de dados para a transferência de dados pessoais para países terceiros, JO L 385, 29.12.2004, p. 74.

11 Decisão 2002/16/CE da Comissão, de 27 de dezembro de 2001, relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, JO L 6, 10.1.2002, p. 52, e 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, JO L 39 de 12.2.2010, p. 5. A decisão anterior, revogada pela atual, aplica-se apenas a contratos celebrados antes de 15 de maio de 2010.

pessoais, e ainda regras sobre a reparação do titular dos dados em caso de danos decorrentes de uma violação por qualquer uma das partes das cláusulas contratuais-tipo. As cláusulas-tipo exigem, igualmente, que o titular de dados da UE tenha a possibilidade de invocar, perante uma autoridade de proteção dedos e/ou um tribunal do Estado-Membro no qual o exportador dos dados está estabelecido, os direitos que decorrem das cláusulas-tipo na qualidade de terceiro beneficiário[12]. Tais direitos e obrigações são necessários nas cláusulas-tipo porque, ao contrário da situação em que a Comissão tenha emitido uma declaração de adequação, não se pode presumir que o importador de dados no país terceiro esteja sujeito a um sistema adequado de supervisão e aplicação das regras em matéria de proteção de dados.

Uma vez que as decisões da Comissão são vinculativas na sua totalidade nos Estados-Membros, a incorporação de cláusulas contratuais-tipo num contrato significa que as autoridades nacionais têm, em princípio, a obrigação de aceitar essas cláusulas. Consequentemente, não podem recusar a transferência de dados para um país terceiro com base apenas no facto de estas cláusulas contratuais-tipo não oferecerem garantias suficientes. Isto sem prejuízo da sua capacidade para examinar as referidas cláusulas à luz dos requisitos definidos pelo Tribunal no acórdão Schrems. Em caso de dúvida, devem intentar uma ação judicial junto de um tribunal nacional que, por sua vez, pode solicitar uma decisão a título prejudicial ao Tribunal de Justiça. Embora não exista nenhuma obrigação de autorização nacional prévia para proceder à transferência na legislação da maioria dos Estados-Membros de transposição da Diretiva 95/45/CE, alguns Estados-Membros mantêm um sistema de notificação e/ou autorização prévia para o recurso a cláusulas contratuais-tipo. Em tal caso, a autoridade de proteção de dados nacional tem de comparar as cláusulas efetivamente contidas no contrato em questão com as cláusulas contratuais-tipo e confirmar que não foi feita qualquer alteração[13]. Se as cláusulas tiverem sido utilizadas sem modificações[14], a autorização é, em princípio[15], automaticamente concedida[16]. Conforme explicado mais em detalhe infra (ver secção 2.4), tal não prejudica as medidas adicionais que o exportador dos dados tenha de tomar, em particular na sequência de informações recebidas do importador dos dados sobre

---

12 Ver, por exemplo, o considerando 6 da Decisão 2004/915/CE da Comissão e a cláusula V do seu anexo; cláusula 7 do anexo à Decisão 2010/87/UE da Comissão.

13 É de notar que a proposta de regulamento geral sobre a proteção de dados [COM(2012) 11 final] prevê que as transferências baseadas em SCC ou BCR não necessitam de qualquer autorização adicional, na medida em que tenham sido adotadas pela Comissão ou de acordo com o mecanismo de coerência pretendido.

14 Contudo, o uso de SCC não impede que as partes acordem aditar outras cláusulas, desde que não sejam contraditórias, de forma direta ou indireta, com as cláusulas aprovadas pela Comissão ou prejudiquem os direitos ou liberdades fundamentais dos titulares dos dados. Ver Comissão Europeia, «Questões mais frequentes relacionadas com transferências de dados pessoais da UE/do EEE para países terceiros» (FAQ B.1.9), p. 28 (disponível na Internet em: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

15 Se uma APD tiver dúvidas quanto à compatibilidade das SCC com os requisitos da Diretiva, deve apresentar a questão a um tribunal nacional que poderá solicitar uma decisão a título prejudicial ao Tribunal de Justiça (cf. n.os 51, 52, 64 e 65 do acórdão Schrems).

16 O Grupo de Trabalho do artigo 29.º estabeleceu um procedimento de cooperação específico entre as autoridades de proteção de dados para a aprovação de cláusulas-tipo que uma empresa procure utilizar em diferentes Estados-Membros. Ver Grupo de Trabalho do artigo 29.º, «Documento de trabalho que define um procedimento de cooperação para a emissão de pareceres comuns em matéria de "cláusulas-tipo" consideradas em conformidade com a cláusula modelo da CE» (WP 226), 26 de novembro de 2014. Ver também a cláusula VII do anexo à Decisão 2004/915/CE da Comissão e a cláusula 10 do anexo à Decisão 2010/87/UE da Comissão.

alterações à ordem jurídica do país terceiro suscetíveis de impedir o importador dos dados de cumprir as suas obrigações ao abrigo do contrato. Na aplicação das cláusulas contratuais-tipo, tanto os exportadores de dados como, por se sujeitarem ao contrato, os importadores de dados, estão sob supervisão das autoridades de proteção de dados.

A adoção das cláusulas contratuais-tipo não impede as empresas de se basearem noutros instrumentos, designadamente os acordos contratuais *ad hoc*, para demonstrar que as suas transferências ocorrem com garantias suficientes na aceção do artigo 26.º, n.º 2, da Diretiva 95/46/CE. Ao abrigo desta última disposição da Diretiva, esses instrumentos têm de ser aprovados caso a caso pelas autoridades nacionais. Algumas autoridades de proteção de dados criaram orientações nesta matéria, incluindo sob a forma de contratos-tipo ou regras pormenorizadas a seguir na redação das cláusulas de transferência de dados. A maioria dos contratos atualmente usados pelas empresas para realizar as suas transferências de dados internacionais baseia-se, contudo, em cláusulas contratuais-tipo aprovadas pela Comissão[17].

## 2.2. Transferências intragrupo

Uma empresa multinacional para transferir dados pessoais da UE para filiais estabelecidas fora da União em conformidade com os requisitos enunciados no artigo 26.º, n.º 2, da Diretiva 95/46/CE, pode adotar regras vinculativas para as empresas (BCR). Este tipo de código de boas práticas só pode servir de base às transferências efetuadas dentro do mesmo grupo empresarial.

O recurso às regras vinculativas para as empresas permite, dessa forma, que os dados pessoais circulem livremente entre as várias entidades de um grupo empresarial em todo o mundo – sem necessidade de dispor de acordos contratuais entre todas e cada uma das entidades da empresa – assegurando, simultaneamente, que se cumpre o mesmo nível elevado de proteção de dados pessoais em todo o grupo por meio de um único conjunto de regras vinculativas e executórias. Dispor de um único conjunto de regras cria um sistema mais simples e eficaz, mais fácil de implementar pelo pessoal e de compreender pelos titulares dos dados. Com vista a ajudar as empresas na elaboração de BCR, o Grupo de Trabalho do artigo 29.º especificou os requisitos materiais (por exemplo, a limitação da finalidade, a segurança do tratamento, informações transparentes para os titulares de dados, restrições relativas a transferências ulteriores fora do grupo, os direitos individuais de acesso, de retificação e de oposição) e processuais (por exemplo, auditorias, controlo da conformidade, tratamento de queixas, cooperação com as autoridades de proteção de dados, responsabilidade e competência) para as BCR, com base em normas de proteção de dados da UE[18]. Estas regras não só são vinculativas para os membros do grupo empresarial mas, tal como acontece com as cláusulas

[17] Ver Grupo de Trabalho do artigo 29.º, «Documento de trabalho que define um procedimento de cooperação para a emissão de pareceres comuns em matéria de "cláusulas-tipo" consideradas em conformidade com a cláusula modelo da CE» (WP 226), 26 de novembro de 2014, p. 2.

[18] Ver Grupo de Trabalho do artigo 29.º, «Documento de trabalho que estabelece uma tabela com os elementos e princípios constantes das regras vinculativas para empresas» (WP 154), 24 de junho de 2008; «Documento de trabalho que estabelece um quadro para a estrutura das regras vinculativas para empresas» (WP 154), 24 de junho de 2008; e «Documento de trabalho sobre as questões mais frequentes (FAQ) relacionadas com as regras vinculativas para empresas» (WP 155), 24 de junho de 2008.

contratuais-tipo, são igualmente executórias na UE: os indivíduos cujos dados estejam a ser tratados por uma entidade do grupo terão o direito, como terceiro beneficiários, a fazer respeitar as BCR, apresentando uma queixa junto de uma autoridade de proteção de dados e intentando uma ação num tribunal de um Estado-Membro. Além disso, as BCR devem designar uma entidade na UE que assuma a responsabilidade pela violação dessas regras por qualquer membro do grupo fora da UE vinculado pelas mesmas.

Ao abrigo da maioria da legislação dos Estados-Membros que transpõe a Diretiva, as transferências de dados com base em BCR têm de ser autorizadas pela autoridade de proteção de dados em cada Estado-Membro a partir do qual a empresa multinacional pretende transferir dados. Para facilitar e acelerar o processo, bem como reduzir o ónus que recai sobre os requerentes, o Grupo de Trabalho do artigo 29.º criou um formulário de pedido normalizado[19] e um procedimento específico de cooperação entre as autoridades de proteção de dados em causa[20] que inclui a designação de uma «autoridade principal» responsável pela gestão do procedimento de aprovação.

## 2.3. Derrogações

Na falta de uma decisão de adequação nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE e independentemente da utilização de cláusulas contratuais-tipo e/ou de regras vinculativas para as empresas, os dados pessoais podem ser transferidos para entidades estabelecidas num país terceiro, na medida em que uma das derrogações alternativas previstas no artigo 26.º, n.º 1, da Diretiva 95/46/CE se aplique[21]:

– O titular dos dados tenha dado de forma inequívoca o seu consentimento à transferência proposta;

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

– A transferência seja necessária à execução ou celebração de um contrato celebrado no interesse do titular dos dados, entre o responsável pelo tratamento e um terceiro;

---

19 Grupo de Trabalho do artigo 29.º, «Modelo de pedido para aprovação das regras vinculativas para empresas aplicáveis à transferência de dados pessoais» (WP 133), 10 de janeiro de 2007.

20 Grupo de Trabalho do artigo 29.º, «Documento de trabalho que estabelece um procedimento de cooperação para a emissão de pareceres comuns sobre garantias adequadas resultantes das "regras vinculativas para empresas"» (WP 107), 14 de abril de 2005.

21 Como o Grupo de Trabalho do artigo 29.º salientou, na medida em que outras disposições da Diretiva 95/46/CE contêm requisitos adicionais pertinentes para a utilização destas exceções (por exemplo, as limitações do artigo 8.º para o tratamento de dados sensíveis), estes devem ser respeitados. Ver Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 8. Ver também Comissão Europeia, «Questões mais frequentes relacionadas com a transferência de dados pessoais da UE/do EEE para países terceiros» (FAQ D.2), p. 50.

– A transferência seja necessária ou legalmente exigida para a proteção de um interesse público importante[22], ou para a declaração, o exercício ou a defesa de um direito num processo judicial;

– A transferência seja necessária para proteger os interesses vitais do titular dos dados;

– A transferência seja realizada a partir de um registo público que, nos termos de disposições legislativas ou regulamentares, se destine à informação do público e se encontre aberto à consulta pelo público em geral ou por qualquer pessoa que possa provar um interesse legítimo, desde que as condições estabelecidas na lei para a consulta sejam cumpridas no caso concreto.

Estes motivos constituem uma derrogação da proibição geral de transferir dados pessoais para entidades estabelecidas num país terceiro sem um nível de proteção adequado. Com efeito, o exportador de dados não tem de assegurar que o importador de dados garantirá uma proteção adequada e, normalmente, não deve obter autorização prévia para a transferência por parte das autoridades nacionais competentes. No entanto, devido ao seu caráter excecional, o Grupo de Trabalho do artigo 29.º considera que estas derrogações devem ser interpretadas de forma restritiva[23].

O Grupo de Trabalho do artigo 29.º emitiu vários documentos de orientação não vinculativos sobre a aplicação do artigo 26.º, n.º 1, da Diretiva 95/46/CE[24]. Estes incluem um certo número de regras em matéria de «melhores práticas» concebidas para orientar a ação das autoridades de proteção de dados[25]. Em particular, o Grupo recomenda que as transferências de dados pessoais consideradas repetidas, volumosas ou estruturais devem ser realizadas com garantias suficientes e, sempre que possível, no âmbito de um quadro jurídico específico, como as cláusulas contratuais-tipo ou regras vinculativas para as empresas[26].

---

22 Tal pode incluir, por exemplo, transferências de dados entre autoridades fiscais ou aduaneiras, ou entre serviços competentes da segurança social (ver considerando 58 da Diretiva 95/46/CE). As transferências entre organismos de supervisão no setor dos serviços financeiros também podem beneficiar da derrogação. Ver Grupo de Trabalho do artigo 29.º, «Documento de trabalho: Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva comunitária relativa à proteção de dados» (WP 12), de 24 de julho de 1998, p. 25.

23 Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, pp. 7 e 17.

24 Grupo de Trabalho do artigo 29.º, «Documento de trabalho: Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva de proteção de dados da UE» (WP 12), 24 de julho de 1998; «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005. Ver também Comissão Europeia, «Questões mais frequentes relacionadas com a transferência de dados pessoais da UE/do EEE para países terceiros» (FAQ D.1 a D.9), pp. 48-54.

25 Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, pp. 8-10.

26 Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 9. Segundo o Grupo de Trabalho, as transferências em massa ou repetidas só podem ser efetuadas com base numa derrogação quando o recurso a SCC ou a BCR é impossível na prática, e os riscos para os titulares dos dados são reduzidos (por exemplo, transferências internacionais de dinheiro). Ver também Comissão Europeia,

Na presente comunicação, a Comissão examina apenas as derrogações que resultam particularmente pertinentes para as transferências no contexto comercial, na sequência da constatação de que a Decisão Porto Seguro foi invalidada.

### 2.3.1. Transferências necessárias para a execução de um contrato ou para a execução de diligências prévias à formação do contrato decididas a pedido do titular dos dados (artigo 26.º, n.º 1, alínea b))

Esta derrogação pode ser aplicável, por exemplo, no contexto de uma reserva de hotel, ou quando as informações relativas ao pagamento são transferidas para um país terceiro para efetuar uma transferência bancária. Todavia, em todos estes casos, o Grupo de Trabalho do artigo 29.º considera que tem de existir uma «relação estreita e substancial», uma «ligação direta e objetiva» entre o titular dos dados e a finalidade do contrato ou da diligência pré-contratual (critério da necessidade)[27]. Além disso, a derrogação não pode ser aplicada a transferências ulteriores de informações desnecessárias para fins da transferência, ou a transferências para uma finalidade diferente da execução do contrato (por exemplo, acompanhamento de uma operação de comercialização)[28]. No que diz respeito às diligências pré-contratuais, o Grupo de Trabalho do artigo 29.º considerou que só os contactos iniciados pelo titular dos dados (por exemplo, um pedido de informações sobre um determinado serviço) seriam abrangidos, mas não os resultantes de estratégias de comercialização efetuadas pelo responsável pelo tratamento de dados[29].

### 2.3.2. Transferências necessárias para a celebração ou execução de um contrato celebrado no interesse do titular dos dados entre o responsável pelo tratamento e um terceiro (artigo 26.º, n.º 1, alínea c))

Esta derrogação pode ser aplicável, por exemplo, quando o titular dos dados é o beneficiário de uma transferência bancária internacional, ou quando uma agência de viagens envia os dados de uma reserva de voo para uma companhia aérea. Uma vez mais, o critério da necessidade aplica-se e, neste caso, requer uma ligação estreita e substancial entre o interesse do titular dos dados e o objetivo pretendido com o contrato.

### 2.3.3. Transferências necessárias ou legalmente exigidas para a declaração, o exercício ou a defesa de um direito num processo judicial (artigo 26.º, n.º 1, alínea d))

---

«Questões mais frequentes relacionadas com a transferência de dados pessoais da UE/do EEE para países terceiros» (FAQ D.1), p. 49.

27 Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 13. Ver também «Parecer 6/2002 sobre a transmissão para os Estados Unidos de informações sobre a lista de passageiros e outros dados provenientes das companhias aéreas» (WP 66), de 24 de outubro de 2002.

28 Grupo de Trabalho do artigo 29.º, «Documento de trabalho: Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva de proteção de dados da UE» (WP 12), 24 de julho de 1998, p. 24; «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 13.

29 Grupo de Trabalho do artigo 29.º, «Documento de trabalho: Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva comunitária relativa à proteção de dados» (WP 12), de 24 de julho de 1998, p. 24.

Esta derrogação pode aplicar-se, por exemplo, quando uma empresa tem de transferir dados para se defender numa ação judicial, ou para apresentar uma ação num tribunal ou perante uma autoridade pública. Tal como para as duas derrogações anteriores, esta está igualmente sujeita ao critério da necessidade[30]: deve existir uma ligação estreita com um litígio ou uma ação judicial (incluindo em matéria administrativa).

Segundo o Grupo de Trabalho do artigo 29.º, a derrogação só pode ser aplicada se as regras sobre cooperação internacional nos processos civis ou penais que regulam o tipo de transferência tiverem sido cumpridas, nomeadamente quando resultam de disposições da Convenção da Haia de 18 de março de 1970 (Convenção sobre Obtenção de Provas)[31].

### 2.3.4. Consentimento prévio inequívoco do titular dos dados à transferência proposta (artigo 26.º, n.º 1, alínea a))

Embora o consentimento possa ser utilizado como base para a transferência de dados, várias considerações devem ser tidas em conta. Uma vez que a transferência «proposta» necessita de consentimento, este deve ser dado previamente para essa transferência em particular (ou para uma categoria particular de transferências). Quando o pedido é solicitado em linha, o Grupo de Trabalho do artigo 29.º recomendou a utilização de caixas a serem sinalizadas pela pessoa (em vez de caixas previamente sinalizadas)[32]. Dado que o consentimento deve ser inequívoco, qualquer dúvida sobre se o mesmo foi efetivamente dado tornaria a derrogação inaplicável. Tal significa provavelmente que muitas situações em que o consentimento é, na melhor das hipóteses, implícito (por exemplo, quando a pessoa teve conhecimento da transferência e não apresentou qualquer objeção), não seriam admissíveis. Em contrapartida, a derrogação pode ser utilizada nos casos em que a entidade que transfere dispõe de um contacto direto com o titular dos dados, quando a informação necessária pode ser facilmente fornecida e o consentimento inequívoco obtido[33].

Além disso, nos termos do artigo 2.º, alínea h), da Diretiva 95/46/CE, o consentimento deve ser dado de forma livre, específica e informada. Segundo o Grupo de Trabalho do artigo 29.º, o primeiro requisito significa que qualquer «pressão» pode invalidar o consentimento. Este

---

30 Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 15. Por exemplo, no contexto laboral, a derrogação não pode ser utilizada para a transferência de todos os ficheiros do empregado para a empresa-mãe do grupo estabelecida num país terceiro com fundamento em eventuais futuras ações judiciais.

31 Convenção da Haia sobre a obtenção de provas no estrangeiro em matéria civil e comercial, *aberta para assinatura* em 18 de março de 1970, 23 U.S.T. 2555, 847 U.N.T.S. 241. Esta convenção abrange, por exemplo, a apresentação de provas previamente ao processo (*pre-trial discovery*) ou pedidos pela autoridade judiciária de um Estado à autoridade competente de outro Estado para obter provas destinadas a serem utilizadas num processo judicial no Estado requerente.

32 Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 10, com referência ao «Parecer 5/2004 sobre as comunicações de marketing direto não solicitadas nos termos do artigo 13.º da Diretiva 2002/58/CE» (WP 90), de 27 de fevereiro de 2004, ponto 3.2.

33 Grupo de Trabalho do artigo 29.º, «Documento de trabalho: Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva comunitária relativa à proteção de dados» (WP 12), de 24 de julho de 1998, p. 24.

aspeto é particularmente relevante no contexto laboral, em que a relação de subordinação e de dependência inerente dos trabalhadores é tal que, em princípio, põe em causa o consentimento[34]. De um modo mais geral, o consentimento de um titular de dados que não teve oportunidade de fazer uma escolha genuína ou foi confrontado com um facto adquirido não pode ser considerado válido[35].

É muito importante que os titulares dos dados sejam informados com a devida antecedência sobre a eventual transferência dos dados para fora da UE, qual o país terceiro destinatário e em que condições (finalidade, identidade e coordenadas do ou dos destinatários, etc.). Estas informações devem mencionar o risco específico de que os dados sejam transferidos para um país terceiro sem um nível de proteção adequado[36]. Além disso, tal como referido pelo Grupo de Trabalho do artigo 29.º, a retirada do consentimento do titular dos dados, embora sem efeitos retroativos, deve, por princípio, impedir a continuação do tratamento dos dados pessoais[37]. À luz destas limitações, o Grupo de Trabalho do artigo 29.º considera que o consentimento não é suscetível de facultar um quadro adequado a longo prazo para os responsáveis pelo tratamento dos dados no caso de transferências estruturais[38].

## 2.4. Resumo sobre as bases alternativas para a transferência de dados pessoais

Decorre do que precede que as empresas podem utilizar vários instrumentos alternativos para efetuar as respetivas transferências internacionais de dados para países terceiros considerados como não garantindo um nível de proteção adequado na aceção do artigo 25.º, n.º 2, da Diretiva 95/46/CE. Na sequência do acórdão Schrems, o Grupo de Trabalho do artigo 29.º esclareceu, nomeadamente, que as cláusulas contratuais-tipo e as BCR podem ser utilizadas para a transferência de dados para os EUA, enquanto prossegue a sua avaliação e sem prejuízo das competências das autoridades de proteção de dados para investigar casos particulares[39]. Por seu lado, a indústria tem reagido de formas diferentes ao acórdão, inclusive baseando as suas transferências de dados nos referidos instrumentos alternativos[40].

---

34 Grupo de Trabalho do artigo 29.º, «Parecer 8/2001 sobre o processamento de dados pessoais no contexto do emprego» (WP 48), 13 de setembro de 2001, pp. 3, 23 e 26. Segundo o Grupo de Trabalho, o recurso ao consentimento deve limitar-se a casos em que o trabalhador disponha de uma verdadeira liberdade de escolha e, consequentemente, possa retirar o seu consentimento sem ser prejudicado. Ver também Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 11.

35 Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 11. Ver também «Parecer 6/2002 sobre a transmissão para os Estados Unidos de informações sobre o registo de passageiros e outros dados provenientes das companhias aéreas» (WP 66), de 24 de outubro de 2002.

36 Grupo de Trabalho do artigo 29.º, «Documento de trabalho: Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Diretiva comunitária relativa à proteção de dados» (WP 12), de 24 de julho de 1998, p. 24.

37 Grupo de Trabalho do artigo 29.º, «Parecer 15/2011 sobre a definição de consentimento» (WP 187), 13 de julho de 2011, p. 9.

38 Grupo de Trabalho do artigo 29.º, «Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995» (WP 114), 25 de novembro de 2005, p. 11.

39 Ver a Declaração do Grupo de Trabalho do artigo 29.º de 16 de outubro de 2015 (nota de rodapé 8, supra).

40 Várias empresas multinacionais declararam basear as suas transferências de dados para os EUA em instrumentos alternativos. Ver, por exemplo, as declarações da Microsoft (http://blogs.microsoft.com/on-the-

Contudo, é necessário salientar duas condições importantes. Em primeiro lugar, importa recordar que, independentemente da base jurídica invocada, as transferências para um país terceiro só podem ser legalmente efetuadas se os dados tiverem sido originalmente recolhidos e tratados pelo responsável pelo tratamento de dados estabelecido na UE em conformidade com a legislação nacional que transpõe a Diretiva 95/46/CE. Este instrumento especifica expressamente que a atividade de tratamento realizada antes da transferência, tal como a própria transferência, deve respeitar plenamente as regras adotadas pelos Estados-Membros nos termos das restantes disposições da Diretiva[41]. Em segundo lugar, na ausência de uma declaração de adequação por parte da Comissão, cabe aos responsáveis pelo tratamento assegurarem que as suas transferências de dados são efetuadas com as garantias suficientes na aceção do artigo 26.º, n.º 2, da Diretiva. Esta avaliação tem de ser realizada tendo em consideração todas as circunstâncias que envolvem a transferência em questão. Em particular, tanto as cláusulas contratuais-tipo como as BCR preveem que, se o importador de dados tiver motivos para crer que a legislação aplicável no país do destinatário o pode impedir de cumprir as suas obrigações, deve desse facto informar imediatamente o exportador de dados na UE. Neste caso, compete ao exportador tomar as medidas adequadas necessárias para assegurar a proteção dos dados pessoais[42]. Tais medidas podem ir desde medidas técnicas, organizacionais, relacionadas com o modelo de negócio ou jurídicas[43], até à possibilidade de suspender a transferência de dados ou rescindir o contrato. Tendo em conta todas as circunstâncias da transferência, os exportadores de dados podem, portanto, ter de aplicar garantias adicionais para complementar as concedidas por força da base jurídica aplicável à transferência a fim de cumprir os requisitos do artigo 26.º, n.º 2 da Diretiva.

O cumprimento desses requisitos deve, em última análise, ser avaliado pelas autoridades de proteção de dados caso a caso, como parte do exercício das respetivas funções de controlo e aplicação, incluindo no contexto da aprovação de acordos contratuais e BCR, ou com base em queixas individuais. Embora algumas autoridades de proteção de dados tenham manifestado dúvidas sobre a possibilidade de utilizar os instrumentos de transferência, como cláusulas contratuais-tipo e BCR, para os fluxos de dados transatlânticos[44], na declaração que emitiu

---

issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) ou da Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). Outras empresas dos EUA, como a Oracle, disseram que oferecem aos clientes de serviços em nuvem a possibilidade de armazenarem os seus dados na Europa, para que os mesmos não sejam enviados para armazenamento noutro local: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot

41 Ver considerando 60 e artigo 25.º, n.º 1, da Diretiva 95/46/CE.

42 Ver, por exemplo, a cláusula 5 do anexo à Decisão 2010/87/UE da Comissão, e Grupo de Trabalho do artigo 29.º, «Documento de trabalho que estabelece um quadro para a estrutura das regras vinculativas para empresas» (WP 154), 24 de junho de 2008, p. 8.

43 Ver, por exemplo, as orientações emitidas pela Agência da União Europeia para a Segurança das Redes e da Informação (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

44 Ver, por exemplo, o documento estratégico publicado pela Conferência da Proteção de Dados das Autoridades de Proteção de Dados Alemãs a Nível Federal e Estatal em 26.10.2015: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521. Salientando que o acórdão Schrems contém «rigorosos requisitos materiais» que tanto a Comissão como as autoridades de proteção de dados têm de

após o acórdão Schrems, o Grupo de Trabalho do artigo 29.º anunciou que irá continuar a sua análise do impacto do acórdão noutros instrumentos de transferência[45]. Isto sem prejuízo das competências das autoridades de proteção de dados para investigar casos particulares e para exercer os respetivos poderes de forma a proteger as pessoas.

## 3. AS CONSEQUÊNCIAS DO ACÓRDÃO SCHREMS SOBRE AS DECISÕES DE ADEQUAÇÃO

No seu acórdão, o Tribunal de Justiça não põe em causa as competências da Comissão nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE para determinar que um país terceiro assegura um nível de proteção adequado, desde que os requisitos estabelecidos pelo Tribunal de Justiça sejam respeitados. Em conformidade com esses requisitos, a proposta de 2012 de um regulamento geral de proteção de dados[46] para substituir a Diretiva 95/46/CE, esclarece e especifica as condições em que podem ser adotadas as decisões de adequação. No acórdão Schrems, o Tribunal também esclareceu que, sempre que a Comissão adote uma decisão de adequação, esta é vinculativa para todos os Estados-Membros e os seus órgãos, incluindo as autoridades de proteção de dados, enquanto não for revogada, anulada ou declarada inválida pelo Tribunal de Justiça, que tem competência exclusiva nesta matéria. As autoridades de proteção de dados mantêm a sua competência no que se refere à apreciação das provas, na aceção do artigo 28.º, n.º 4, da Diretiva 95/46/CE, de que a transferência de dados cumpre os requisitos estipulados pela diretiva (na interpretação que lhe é dada pelo Tribunal de Justiça), mas não podem emitir uma decisão definitiva sobre a matéria. Em vez disso, os Estados-Membros têm de prever a possibilidade de apresentar a ação a um tribunal nacional que, por sua vez, pode recorrer à competência do Tribunal de Justiça mediante um pedido de decisão a título prejudicial, nos termos do artigo 267.º do Tratado sobre o Funcionamento da União Europeia (TFUE).

---

respeitar, o documento indica que as autoridades de proteção de dados alemãs irão avaliar a licitude das transferências de dados com base em instrumentos alternativos (SCC, BCR) e deixar de conceder novas autorizações para a utilização destes instrumentos. Paralelamente, autoridades de proteção de dados alemãs individuais emitiram avisos claros de que os instrumentos de transferência alternativos são objeto de apreciação jurídica. Ver, por exemplo, os documentos estratégicos emitidos pelas autoridades de proteção de dados de Schleswig-Holstein: https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html e de Rheinland-Pfalz: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

45 Ver a Declaração do Grupo de Trabalho do artigo 29.º de 16 de outubro de 2015 (nota de rodapé 8 supra).

46 Comissão Europeia, proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados). Ver também Parlamento Europeu, Resolução legislativa, de 12 de março de 2014, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), COM(2012)0011 – C7-0025/2012-2012/0011 (COD); Conselho, proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), Preparação de uma orientação geral, 9565/15. A proposta está atualmente na fase final do processo legislativo.

Além disso, o Tribunal de Justiça confirmou expressamente que o recurso, por parte de um país terceiro, a um sistema de autocertificação (como no caso dos princípios de «porto seguro») não exclui uma decisão de adequação nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE, enquanto houver mecanismos eficazes de deteção e supervisão que permitam, na prática, identificar e sancionar qualquer violação das regras de proteção de dados.

Tendo em conta que a Decisão Porto Seguro não continha elementos suficientes a este respeito, o Tribunal de Justiça declarou a decisão inválida. É, por conseguinte, claro que as transferências de dados entre a UE e os Estados Unidos não podem continuar a ser efetuadas nessa base, ou seja, invocando unicamente a adesão aos princípios de «porto seguro». Uma vez que as transferências de dados para um país terceiro que não assegure um nível de proteção adequado (ou, pelo menos, nos casos em que tal não tenha sido estabelecido numa decisão da Comissão na aceção do artigo 25.º, n.º 6, da Diretiva 95/46/CE) são, em princípio, proibidas[47], só serão lícitas se o exportador dos dados puder basear-se num dos instrumentos alternativos descritos na secção 2. Na ausência de uma decisão de adequação, é da responsabilidade do exportador dos dados – sob controlo das autoridades de proteção de dados – assegurar que as condições para recorrer a algum desses instrumentos foram cumpridas no que se refere à transferência de dados.

O âmbito do acórdão está limitado à Decisão Porto Seguro da Comissão. Contudo, cada uma das restantes decisões de adequação[48] contém uma restrição aos poderes das autoridades de proteção de dados idêntica ao artigo 3.º da referida decisão e que o Tribunal de Justiça considerou inválida[49]. A Comissão irá agora retirar as necessárias consequências do acórdão, preparando em breve uma decisão a adotar nos termos do procedimento de comitologia aplicável, visando substituir essa disposição em todas as decisões de adequação existentes. Além disso, a Comissão realizará uma avaliação regular das decisões de adequação existentes e futuras, inclusive através da revisão conjunta periódica do respetivo funcionamento, em colaboração com as autoridades competentes do país terceiro em questão.

## 4. CONCLUSÃO

Como confirmado pelo Grupo de Trabalho do artigo 29.º, os instrumentos alternativos que autorizam os fluxos de dados podem ainda ser utilizados pelas empresas para transferirem licitamente dados para países terceiros, como os Estados Unidos. Contudo, a Comissão considera que um quadro renovado e sólido para a transferência de dados pessoais para os Estados Unidos continua a ser uma prioridade crucial. Esse quadro constitui a solução mais completa para assegurar a continuidade efetiva da proteção dos dados pessoais dos cidadãos europeus quando são transferidos para os Estados Unidos. Além disso, constitui a melhor solução para o comércio transatlântico, uma vez que proporciona um mecanismo de

47 Ver considerando 57 da Diretiva 95/46/CE.

48 Atualmente, foram adotadas decisões de adequação relativamente aos seguintes países: Andorra, Argentina, Canadá, Guernesey, Ilha de Man, Ilhas Faroé, Israel, Jersey, Nova Zelândia, Suíça e Uruguai. Ver: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

49 Ver parágrafos 99-104 do acórdão Schrems.

transferência mais simples, menos complexo e, por isso, menos dispendioso, em particular para as PME.

Já em 2013, a Comissão encetou negociações com o Governo dos EUA quanto a um novo acordo para transferências de dados transatlânticas baseado nas suas 13 recomendações[50]. Registaram-se progressos consideráveis na aproximação dos pontos de vista de ambas as partes, por exemplo relativamente ao reforço do controlo e da aplicação dos princípios de «porto seguro», respetivamente, pelo Departamento do Comércio dos Estados Unidos e pela Comissão Federal do Comércio dos Estados Unidos, uma maior transparência para os consumidores quanto aos seus direitos em matéria de proteção de dados, possibilidades de reparação menos complexas e menos onerosas em caso de queixas, bem como regras mais claras sobre as transferências ulteriores a partir de empresas signatárias dos princípios de «porto seguro» para empresas não signatárias destes princípios (por exemplo, para fins de tratamento ou de subtratamento). Agora que a Decisão Porto Seguro foi declarada inválida, a Comissão intensificou as conversações com o Governo dos EUA para assegurar que os requisitos jurídicos formulados pelo Tribunal são respeitados. O objetivo da Comissão é concluir os debates e alcançar este objetivo no prazo de três meses.

Até o quadro transatlântico renovado se encontrar implementado, as empresas necessitam de utilizar os instrumentos alternativos disponíveis. Contudo, esta opção envolve responsabilidades para os exportadores de dados, sob supervisão das autoridades de proteção de dados.

Ao contrário de uma situação em que a Comissão tenha concluído que um país terceiro assegura um nível de proteção adequado de dados no qual os exportadores de dados podem confiar para as transferências de dados da UE, estes últimos continuam a ser responsáveis por verificar se os dados pessoais estão, efetivamente, protegidos quando recorrem a instrumentos alternativos. Tal pode incluir a necessidade de tomarem medidas adequadas, quando necessário.

Neste aspeto, as autoridades de proteção de dados têm um papel central a desempenhar. Na qualidade de principais entidades responsáveis pela aplicação dos direitos fundamentais dos titulares dos dados, as autoridades de proteção de dados são simultaneamente responsáveis e têm poderes para supervisionar as transferências de dados da UE para países terceiros, de forma totalmente independente. A Comissão convida os responsáveis pelo tratamento de dados a cooperarem com as autoridades de proteção de dados, ajudando-as a desempenhar eficazmente as suas funções de supervisão. A Comissão continuará a trabalhar em estreita colaboração com o Grupo de Trabalho do artigo 29.º para assegurar a aplicação uniforme da legislação europeia sobre a proteção de dados.

[50] Ver nota de rodapé 4 supra.