Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
YVES BOT
apresentadas em 23 de setembro de 2015 [1]

Processo C-362/14

Maximillian Schrems
contra
Data Protection Commissioner

[pedido de decisão prejudicial apresentado pela High Court (Irlanda)]

«Reenvio prejudicial — Dados pessoais — Proteção das pessoas singulares no que diz respeito ao tratamento desses dados — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.°, 8.° e 47.° — Diretiva 95/46/CE — Artigo 25.° — Decisão 2000/520/CE — Transferência de dados pessoais para os Estados Unidos — Avaliação do caráter adequado ou não do nível de proteção — Queixa de uma pessoa singular cujos dados foram transferidos para um país terceiro — Autoridade nacional de controlo — Poderes»

I – **Introdução**

1. Como a Comissão Europeia constatou na sua Comunicação de 27 de novembro de 2013 [2], «[a]s transferências de dados pessoais são um elemento importante e necessário da relação transatlântica. Fazem parte integrante das trocas comerciais transatlânticas, nomeadamente nos novos setores digitais emergentes, como as redes sociais ou a computação em nuvem, implicando a transferência de uma grande quantidade de dados da UE para os EUA» [3].

2. As trocas comerciais constituem o objeto da Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América [4]. Esta decisão constitui a base jurídica das transferências de dados pessoais da UE para empresas sedeadas nos EUA que tenham subscrito os princípios de privacidade do sistema «porto seguro».

3. A referida decisão é hoje confrontada com o desafio que consiste em permitir os fluxos de dados entre a União e os Estados Unidos, garantindo um elevado nível de proteção desses dados, como o direito da União exige.

1 — Língua original: francês.

2 — 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].

3 — P. 2.

4 — JO L 215, p. 7; retificação no JO 2001, L 115, p. 14.

4. Com efeito, algumas revelações denunciaram recentemente a existência de programas americanos de recolha de informação em grande escala. Essas revelações lançaram a confusão sobre o respeito das normas do direito da União quando das transferências de dados pessoais para empresas sedeadas nos Estados Unidos e sobre as fragilidades do sistema «porto seguro».

5. O presente reenvio prejudicial convida o Tribunal de Justiça a precisar qual a atitude que as autoridades nacionais de controlo e a Comissão devem adotar quando confrontadas com disfunções na aplicação da Decisão 2000/520.

6. A 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 [5], prevê, no seu capítulo IV, regras sobre a transferência de dados pessoais para países terceiros.

7. Neste capítulo, o artigo 25.º, n.º 1, desta diretiva estabelece o princípio de que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se o país terceiro em questão assegurar um nível de proteção adequado a esses dados.

8. Em contrapartida, como o legislador da União indica no considerando 57 da referida diretiva, sempre que um país terceiro não ofereça um nível de proteção adequado, a transferência de dados pessoais para esse país deve ser proibida.

9. Nos termos do artigo 25.º, n.º 2, da Diretiva 95/46 «[a] adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou setoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país».

10. Em conformidade com o artigo 25.º, n.º 6, desta diretiva, a Comissão pode constatar que um país terceiro assegura, um nível de proteção adequado aos dados pessoais, em virtude da sua legislação interna ou dos seus compromissos internacionais. A partir do momento em que a Comissão adote uma decisão nesse sentido, pode fazer-se a transferência de dados pessoais para o país terceiro em causa.

11. Aplicando esta disposição, a Comissão adotou a Decisão 2000/520. Resulta do artigo 1.º, n.º 1, desta decisão que os «princípios da privacidade em 'porto seguro'», aplicados em conformidade com a orientação que proporcionam as «questões mais frequentes» [6], asseguram um nível de proteção adequado dos dados pessoais transferidos a partir da União para empresas estabelecidas nos Estados Unidos da América.

12. Em consequência, a Decisão 2000/520 autoriza a transferência de dados pessoais a partir dos Estados-Membros para empresas estabelecidas nos Estados Unidos da América que se comprometeram a respeitar os princípios de porto seguro.

13. A Decisão 2000/520 enuncia, no seu anexo I, alguns princípios que as empresas podem subscrever voluntariamente, sujeitos a limites e a um sistema de fiscalização específico. O número de empresas que subscreveram aquilo que se podia qualificar de «código de conduta» ultrapassava as 3 200 em 2013.

5 — JO L 281, p. 31. Diretiva conforme alterada pelo Regulamento (CE) n.º 1882/2003 do Parlamento Europeu e do Conselho, de 29 de outubro de 2003 (JO L 284, p. 1, a seguir «Diretiva 95/46»).

6 — Frequently asked questions (a seguir «FAQ»).

14. O sistema «porto seguro» assenta numa solução mista de autocertificação e de autoavaliação pelas empresas privadas e pela intervenção do poder público.

15. Os princípios de «porto seguro» foram desenvolvidos com base «em consultas ao setor e ao público em geral para facilitar as relações comerciais e as transações entre os Estados Unidos e a União [...]. Destinam-se a ser utilizados exclusivamente por organizações dos EUA que recebam dados pessoais da União [...] para efeitos de reconhecimento como 'porto seguro' e para a presunção de 'adequação' implicada nesse processo» [7].

16. Os princípios de «porto seguro», que figuram no anexo I da Decisão 2000/520, preveem, nomeadamente,

— uma obrigação de informação segundo a qual «[u]ma organização deve informar os cidadãos quanto aos fins a que se destinam a recolha e utilização dos dados que lhes dizem respeito, à forma de contactar a organização para qualquer questão ou queixa, aos tipos de terceiros a quem a informação é comunicada e às opções e meios que a organização coloca à disposição dos cidadãos para limitarem a utilização e comunicação desses dados. Este aviso deve ser formulado […] no momento em que se solicita pela primeira vez qualquer informação pessoal aos cidadãos ou então logo que possível, mas, em qualquer circunstância, antes de a organização utilizar esses dados para outro fim diferente daquele que, inicialmente, motivou a recolha ou o tratamento por parte da entidade que procedeu à transferência, ou ainda antes de a organização divulgar, pela primeira vez, esses dados a terceiros» [8];

— uma obrigação da organização facultar aos cidadãos a possibilidade de escolher («opt out» — opção de não participação) se os seus dados pessoais podem: a) ser divulgados a terceiros, ou b) ser utilizados para fins incompatíveis com os que presidiram à recolha inicial ou com os que foram subsequentemente autorizados pela pessoa em causa. Tratando-se de dados sensíveis, «os cidadãos devem poder exercer uma escolha afirmativa ou explícita no sentido da participação («opt in»), caso se pretenda divulgar a informação a terceiros ou utilizá-la para um fim diferente do que, inicialmente, motivou a sua recolha ou do fim subsequentemente autorizado pela pessoa através do exercício da opção de participação» [9];

— regras relativas à retransferência dos dados. Assim, para poderem divulgar informação a terceiros, as organizações deverão aplicar os princípios de aviso e escolha» [10];

— relativamente à segurança dos dados, uma obrigação de «[a]s organizações que criam, mantêm, utilizam ou divulgam ficheiros de informações pessoais [...] tomar precauções razoáveis para evitar a perda, utilização indevida e acesso, revelação, alteração ou destruição não autorizados» [11];

— quanto à integridade dos dados, uma obrigação das organizações, «[n]a medida necessária para se atingirem [os] fins [para os quais os dados foram recolhidos], […] tomar[em] providências razoáveis para assegurar que os dados são fiáveis para a utilização prevista, exatos, completos e atuais» [12];

7 — Segundo parágrafo do anexo I, da Decisão 2000/520.

8 — V. anexo I, sob «Aviso».

9 — V. anexo I, sob «Escolha».

10 — V. anexo I, sob «Retransferência».

11 — V. anexo I, sob «Segurança».

12 — V. anexo I, sob «Integridade dos dados».

— que os cidadãos cujos dados são detidos por uma organização devem em princípio «ter acesso às informações pessoais que lhes dizem respeito e [...] devem poder retificar, alterar ou eliminar informações inexatas» [13];

— uma obrigação de prever «mecanismos que garantam o cumprimento dos princípios de 'porto seguro', recursos para os cidadãos a que se referem os dados e que tenham sido afetados pelo incumprimento dos princípios, bem como consequências para as organizações sempre que os princípios não sejam seguidos» [14].

17. Uma organização americana que queira aderir aos princípios de «porto seguro» tem de prever, na sua política de proteção da vida privada, que torna público o facto de que adere a esses princípios e que se conforma efetivamente com eles e que se autocertifica declarando ao Ministério do Comércio dos Estados Unidos que está em conformidade com os referidos princípios [15].

18. As organizações dispõem de diversos meios para se conformarem com os princípios de «porto seguro». Assim, podem, por exemplo, «[associar-se] a um programa de autorregulamentação para a proteção da vida privada que adira a estes princípios» ou «desenvolv[er] as suas próprias políticas autorreguladoras de proteção da vida privada, desde que ajam em conformidade com os referidos princípios [do porto seguro]». «Ademais, as organizações regidas por disposições legais, regulamentares, administrativas ou de qualquer outra natureza jurídica que protejam efetivamente a privacidade dos dados pessoais podem candidatar-se aos benefícios do 'porto seguro'» [16].

19. Existem vários mecanismos, que conjugam a arbitragem privada com a fiscalização pelos poderes públicos, para verificar o respeito dos princípios de «porto seguro». Assim, a fiscalização pode ser assegurada por intermédio de um sistema de regulamentação extrajudicial dos litígios por um terceiro independente. Por outro lado, as empresas podem comprometer-se a cooperar com o painel da União sobre a proteção de dados. Por último, a Federal Trade Commission (Comissão Federal do Comércio) (a seguir «FTC»), com base nos poderes que lhe foram conferidos nos termos da section 5 do Federal Trade Commission Act (Lei relativa à Comissão Federal do Comércio), e o Department of Transportation (Ministério dos Transportes) com base nos poderes que lhe foram conferidos nos termos da section 41712 do United States Codes (Código dos Estados Unidos) que figura no seu título 49, são competentes para tratar das queixas.

20. Nos termos do quarto parágrafo do anexo I da Decisão 2000/520, a adesão aos princípios de «porto seguro» pode ser limitada, nomeadamente, na medida necessária para observar «requisitos de segurança nacional, interesse público ou execução legal» e por «legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores avançados por essa autorização» [17].

21. Além disso, a possibilidade de as autoridades competentes dos Estados-Membros suspenderem o fluxo de dados está sujeita a várias condições previstas no artigo 3.º, n.º 1, da Decisão 2000/520.

13 — V. anexo I, sob «Acesso».

14 — V. anexo I, sob «Aplicação».

15 — Artigo 1.º, n.os 2 e 3, da Decisão 2000/530. V., também, anexo II, FAQ 6.

16 — Terceiro parágrafo do anexo I.

17 — V., também, anexo IV, B.

22. O presente pedido de decisão prejudicial leva a questionar o alcance da Decisão 2000/520, à luz dos artigos 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»), e dos artigos 25.°, n.º 6, e 28.º da Diretiva 95/46. Este pedido foi apresentado no âmbito de um litígio que opõe M. Schrems ao Data Protection Commissioner (Comissário para a proteção de dados, a seguir «Comissário»), pelo facto de este último ter recusado investigar uma queixa apresentada por M. Schrems por causa de a Facebook Ireland Ltd. (a seguir «Facebook Ireland») conservar os dados pessoais dos seus utilizadores em servidores situados nos Estados Unidos.

23. M. Schrems é um cidadão austríaco e reside na Áustria. É utilizador da rede social Facebook desde 2008.

24. É pedido a todos os utilizadores do Facebook residentes em território da União para subscreverem um contrato com a Facebook Ireland que é uma filial da sociedade-mãe Facebook Inc., com sede nos Estados Unidos (a seguir «Facebook USA»). Os dados dos utilizadores da Facebook Ireland que residem em território da União são, no todo ou em parte, transferidos para servidores da Facebook USA, situados em território dos Estados Unidos, onde são conservados.

25. Em 25 de junho de 2013, M. Schrems apresentou uma queixa ao Comissário, em que alegava, em substância, que o direito e a prática dos Estados Unidos não asseguram nenhuma proteção real dos dados conservados em seu território contra a vigilância do Estado. Isto resulta das revelações feitas a partir de maio de 2013 por Edward Snowden sobre as atividades dos serviços de informação americanos e, em particular, da National Security Agency (Agência Nacional de Segurança) (a seguir «NSA»).

26. Resulta, designadamente, dessas revelações que a NSA tinha estabelecido um programa denominado «PRISM» no âmbito do qual esta agência tinha obtido livre acesso a grandes volumes de dados armazenados nos servidores localizados nos Estados Unidos, na posse ou controlados por um conjunto de sociedades ativas nos domínios da Internet e da tecnologia, como a Facebook USA.

27. O Comissário considerou que não estava obrigado a investigar a queixa, na medida em que esta não tinha fundamento jurídico. Considerou que não havia provas de que a NSA tivesse acesso aos dados de M. Schrems. Além disso, na sua opinião, a queixa devia ser rejeitada por força da Decisão 2000/520 pela qual a Comissão constatou que os Estados Unidos asseguram, no âmbito do sistema «porto seguro», um nível de proteção adequado dos dados pessoais transferidos. Qualquer questão relativa ao caráter adequado da proteção desses dados nos Estados Unidos devia ser decidida em conformidade com esta decisão que o impedia de analisar o problema suscitado pela queixa.

28. A legislação nacional que levou o Comissário rejeitar a queixa é a seguinte.

29. O artigo 10.º, n.º 1, do Data Protection Act 1988 (Lei de 1988 sobre a proteção de dados) conforme alterado pelo Data Protection (Amendment) Act 2003 (Lei de 2003 sobre a proteção de dados (a seguir «Lei sobre a proteção de dados») confere-lhe o poder de analisar as queixas e enuncia:

«a) O Comissário pode analisar ou mandar analisar se as disposições da presente lei foram, são ou podem ser infringidas em relação a uma determinada pessoa, quer porque essa pessoa lhe apresenta queixa por infração a qualquer uma dessas disposições, quer porque este considera que essa infração possa existir.

b) Quando uma pessoa apresenta queixa ao Comissário nos termos da alínea a) do presente número, este:

i) instrui ou manda instruir a queixa, salvo se concluir que esta é frívola ou ultrajante, e,

ii) se, num prazo razoável, não puder obter das partes em questão um acordo amigável sobre o objeto da queixa, avisa por escrito o queixoso da decisão que tomar sobre a mesma, referindo que, se essa decisão lhe for desfavorável, o queixoso pode interpor recurso judicial ao abrigo do artigo 26.º da presente lei, num prazo de 21 dias a contar da receção da notificação.»

30. No caso em apreço, o Comissário decidiu que a queixa de M. Schrems era «frívola ou ultrajante» pelo que estava votada ao insucesso uma vez que era desprovida de fundamento jurídico. Foi nestes termos que se recusou a instruir esta queixa.

31. O artigo 11.º da Lei sobre a proteção de dados regula a transferência de dados pessoais para fora do território nacional. O artigo 11.º, n.º 2, alínea a), desta lei prevê:

«Quando, em qualquer processo regulado pela presente lei, for suscitada uma questão:

i) para determinar se o nível de proteção adequado estabelecido no n.º 1 do presente artigo é assegurado por um país ou um território fora do Espaço Económico Europeu [(EEE)] para onde vão ser transferidos os dados pessoais, e

ii) a União fez uma constatação relativamente ao tipo de transferência em causa,

a questão será decidida em conformidade com essa constatação.»

32. O artigo 11.º, n.º 2, alínea b), da Lei sobre a proteção de dados define o conceito de constatação da União nos seguintes termos:

«Na alínea a) do presente número 'constatação da União' significa uma constatação que a Comissão [...] fez para efeitos do n.º 4 ou do n.º 6 do artigo 25.º da Diretiva [95/46] no âmbito do processo previsto no [seu] artigo 31.º, n.º 2, para determinar se o nível de proteção adequado estabelecido no n.º 1 do presente artigo é assegurado por um país ou território fora do [EEE].»

33. O Comissário observou que a decisão 2000/520 era uma «constatação da União» para efeitos do artigo 11.º, n.º 2, alínea a), da Lei sobre a proteção de dados, de forma que, nos termos dessa lei, qualquer questão relativa ao caráter adequado da proteção dos dados no país terceiro para onde são transferidos devia ser decidida em conformidade com essa constatação. Na medida em que se tratava da questão fundamental da queixa de M. Schrems, a saber, que eram transferidos dados pessoais para um país terceiro que, na prática, não assegurava um nível de proteção adequado, o Comissário considerou que natureza e a existência da própria Decisão 2000/520 o impediam de analisar esta questão.

34. M. Schrems interpôs recurso para a High Court (Supremo Tribunal de Justiça), da decisão do Comissário que rejeitou a sua queixa. Depois de ter analisado as provas apresentadas no processo principal, o referido órgão jurisdicional declarou que a vigilância eletrónica e a interceção de dados pessoais prosseguem fins necessários e indispensáveis de interesse público, a saber a manutenção da segurança nacional e a prevenção de crimes graves. A este propósito, a High Court afirma que a vigilância e a interceção de dados pessoais da União para os Estados Unidos servem objetivos legítimos associados à luta contra o terrorismo.

35. Segundo este mesmo órgão jurisdicional, as revelações feitas por E. Snowden demonstraram, no entanto, que a NSA e outros organismos semelhantes tinham cometido excessos consideráveis. Embora o Foreign Intelligence Services Court (tribunal encarregado de supervisionar os pedidos e mandatos em matéria de vigilância) a seguir «FISC»), que intervém no âmbito do Foreign Intelligence

Surveillance Act of 1978 [18] (Lei de 1978 relativa à vigilância dos serviços de informação estrangeiros), exerça uma supervisão, o processo que lhe é submetido é, todavia, secreto e não contraditório. Acresce que, além do facto de as decisões relativas ao acesso aos dados pessoais serem proferidas com fundamento no direito americano, os cidadãos da União não têm nenhum direito efetivo de serem ouvidos sobre a questão da vigilância e da interceção dos seus dados.

36. Resulta claramente dos volumosos documentos que acompanham as declarações solenes prestadas no processo principal que a exatidão de inúmeras declarações de E. Snowden não é posta em causa. Consequentemente, a High Court declarou que, uma vez que os dados pessoais são transferidos para os Estados Unidos, a NSA e outras agências de segurança americanas como o Federal Bureau of Investigation (FBI) (Gabinete Federal de Investigação) podem aceder aos mesmos no âmbito da vigilância e interceções em larga escala indiferenciadas.

37. A High Court observa que, no direito irlandês, a importância dos direitos constitucionais à vida privada e à inviolabilidade do domicílio exige que qualquer ingerência nesses direitos respeite os requisitos previstos na lei e que seja proporcionada. O acesso em larga escala e indiferenciado a dados pessoais não responde a nenhuma exigência de proporcionalidade e devia, por conseguinte, ser considerado contrário à Constituição irlandesa [19].

38. A High Court salienta que, para que a interceção de comunicações eletrónicas possa ser considerada constitucional, é preciso demonstrar que determinadas interceções de comunicações e a vigilância de certas pessoas ou de certos grupos de pessoas são objetivamente justificadas no interesse da segurança nacional e da repressão da criminalidade e que existem garantias adequadas e verificáveis.

39. Consequentemente, a High Court refere que, se o presente processo fosse apreciado apenas com fundamento no direito irlandês, colocar-se-ia um problema grave quanto à questão de saber se os Estados Unidos «asseguram um nível de proteção adequado da vida privada e das liberdades e dos direitos fundamentais», na aceção do artigo 11.º, n.º 1, da Lei sobre a proteção de dados. Daqui decorre que, com fundamento no direito irlandês, e em particular nos seus requisitos constitucionais, o Comissário não podia ter rejeitado a queixa de M. Schrems devendo, pelo contrário, ter analisado essa questão.

40. Todavia, a High Court constata que o processo, sobre o qual foi chamada a pronunciar-se, tem por objeto a aplicação do direito da União, na aceção do artigo 51.º, n.º 1, da Carta, de modo que a legalidade da decisão do Comissário deve ser apreciada à luz do direito da União.

41. O problema com o qual o Comissário se encontra confrontado é explicado da seguinte forma pela High Court. Nos termos do artigo 11.º, n.º 2, alínea a) da Lei sobre a proteção de dados, o Comissário está obrigado a decidir a questão do caráter adequado da proteção no país terceiro «em conformidade» com uma constatação da União feita pela Comissão ao abrigo do artigo 25.º, n.º 6, da Diretiva 95/46. Daqui resulta que o Comissário não podia afastar-se dessa constatação. Tendo a Comissão concluído na sua Decisão 2000/520, que os Estados Unidos garantiam um nível de proteção adequado em relação ao tratamento de dados pelas sociedades que aderiram aos princípios do porto seguro, uma queixa que invoque o caráter inadequado dessa proteção devia necessariamente ser indeferida pelo Comissário.

18 — V. section 702 deste Act, conforme alterado pelo Foreign Intelligence Surveillance Act of 2008. É ao abrigo desta disposição que a NSA possui uma base de dados conhecida pelo nome de «PRISM» (v. report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, de 27 de novembro de 2013).

19 — A High Court faz referência, em especial, ao respeito pela dignidade humana e à liberdade da pessoa (preâmbulo), à autonomia pessoal (artigo 40.º, n.º 3, pontos 1 e 2), à inviolabilidade do domicílio (artigo 40.º, n.º 5) e à proteção da vida familiar (artigo 41.º).

42. Constatando que o Comissário demonstrou uma fidelidade escrupulosa à letra da Diretiva 95/46 e da Decisão 2000/520, a High Court salienta que M. Schrems na realidade põe mais em causa os termos do próprio sistema de porto seguro do que a forma como o Comissário o aplica, salientado que este não verificou diretamente a validade da Diretiva 95/46 nem da Decisão 2000/520.

43. Por conseguinte, segundo a High Court, a questão essencial é saber se, no que se refere ao direito da União e tendo em conta, em especial, a entrada em vigor posterior dos artigos 7.° e 8.° da Carta, o Comissário está absolutamente vinculado pela constatação da Comissão enunciada na Decisão 2000/520 relativa ao caráter adequado do direito e da prática em matéria de proteção dos dados pessoais nos Estados Unidos.

44. Além disso, a High Court esclarece que, no recurso que lhe foi submetido, não foi feita nenhuma alegação a respeito das ações da Facebook Ireland e da Facebook USA enquanto tais. Ora, o artigo 3.º, n.º 1, alínea b), da Decisão 2000/520, que permite que as autoridades nacionais competentes ordenem a uma empresa que suspenda o fluxo de dados para um país terceiro, só é aplicável, segundo este órgão jurisdicional, em circunstâncias em que a queixa é dirigida contra o comportamento da empresa em causa, o que não se verifica no caso em apreço.

45. Consequentemente, a High Court sublinha que a verdadeira objeção não é dirigida contra o comportamento da Facebook USA enquanto tal, mas contra o facto de a Comissão considerar que o direito e a prática em matéria de proteção de dados nos Estados Unidos garantem uma proteção adequada, quando as revelações de E. Snowden mostram claramente que as autoridades americanas podem aceder em larga escala e de forma indiferenciada aos dados pessoais da população que vive em território da União [20].

46. Neste ponto, a High Court considera que é difícil conceber como é que a Decisão 2000/520 pode, na prática, cumprir os requisitos dos artigos 7.° e 8.° da Carta, *a fortiori* se se tiverem em conta os princípios formulados pelo Tribunal de Justiça no seu acórdão Digital Rights Ireland e o. [21]. Em particular, a garantia prevista no artigo 7.º da Carta, e pelos valores essenciais comuns às tradições dos Estados-Membros, ficaria comprometida se fosse permitido aos poderes públicos terem acesso aleatório e generalizado às comunicações eletrónicas sem terem de dar uma motivação objetiva fundada em razões de segurança nacional ou de prevenção da criminalidade ligadas especialmente a determinados indivíduos e sem nenhuma garantia adequada e verificável. Como o recurso de M. Schrems sugeria que a Decisão 2000/520 poderia, *in abstracto*, ser incompatível com os artigos 7.° e 8.° da Carta, o Tribunal de Justiça podia considerar que é possível interpretar a Diretiva 95/46, e nomeadamente o seu artigo 25.º, n.º 6, bem como a Decisão 2000/520 num sentido que permita às autoridades nacionais conduzir as suas próprias investigações para estabelecer se a transferência de dados pessoais para um país terceiro satisfaz as exigências que decorrem dos artigos 7.° e 8.° da Carta.

47. Foi nestas circunstâncias que a High Court decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«Tendo em conta os artigos 7.°, 8.° e 47.° da Carta [...] e sem prejuízo das disposições do artigo 25.º, n.º 6, da Diretiva 95/46, o Comissário no âmbito da análise de uma queixa segundo a qual o direito e as práticas de um país terceiro (neste caso, os Estados Unidos da América) para o qual são enviados dados pessoais não oferecem proteção adequada, está vinculado em termos absolutos pela constatação em sentido contrário da União, contida na Decisão [...] 2000/520?

20 — A este propósito, a High Court refere que o principal fundamento invocado por M. Schrems perante si consiste em afirmar que, atendendo às recentes declarações de E. Snowden e ao facto de os dados pessoais terem sido postos à disposição dos serviços de informação dos Estados Unidos em grande escala, o Comissário não podia concluir validamente que nesse país terceiro existe um nível de proteção adequado desses dados.

21 — C-293/12 e C-594/12, EU:C:2014:238, n.ºs 65 a 69.

Em alternativa, [este] pode e/ou deve proceder à sua própria investigação sobre a matéria, à luz dos últimos desenvolvimentos de facto ocorridos desde a primeira publicação da [Decisão 2000/502]»?

II – **Análise**

48. As duas questões formuladas pela High Court convidam o Tribunal de Justiça a precisar os poderes de que dispõem as autoridades nacionais de controlo quando chamadas a pronunciar-se sobre uma queixa relativa a uma transferência de dados pessoais para uma empresa sedeada num país terceiro e que alegou, em apoio dessa queixa, que esse país terceiro não garante um nível de proteção adequado aos dados transferidos, quando a Comissão, com fundamento no artigo 25.º, n.º 6, da Diretiva 95/46, tenha aprovado uma decisão que reconhece a adequação do nível de proteção assegurado pelo referido país terceiro.

49. Observo que a queixa apresentada por M. Schrems ao Comissário comporta uma dupla dimensão. Visa contestar a transferência de dados pessoais da Facebook Ireland para a Facebook USA. M. Schrems pede que seja posto termo a essa transferência na medida em que, na sua opinião, os Estados Unidos não asseguram um nível de proteção adequado aos dados pessoais que são transferidos no âmbito do sistema «porto seguro». Mais precisamente, critica este país terceiro por ter implementado o programa PRISM que permite à NSA aceder livremente aos dados em larga escala armazenados nos servidores localizados nos Estados Unidos. Assim, a queixa diz especificamente respeito às transferências de dados pessoais da Facebook Ireland para a Facebook USA pondo em causa de uma forma mais geral o nível de proteção assegurado a esses dados pelo sistema «porto seguro».

50. O Comissário considerou que a própria existência de uma decisão da Comissão que reconhece que os Estados Unidos asseguram, no âmbito do sistema «porto seguro», um nível de proteção adequado, o impedia proceder a investigações sobre a queixa.

51. Importa, assim, analisar em conjunto as duas questões que, em substância, pretendem saber se o artigo 28.º da Diretiva 95/46, lido à luz dos artigos 7.° e 8.° da Carta, deve ser interpretado no sentido de que a existência de uma decisão adotada pela Comissão com fundamento no artigo 25.º, n.º 6, desta diretiva, tem por efeito impedir uma autoridade nacional de controlo de investigar uma queixa que revela que um país terceiro não assegura um nível de proteção adequado aos dados pessoais transferidos e, se for caso disso, suspender a transferência desses dados.

52. O artigo 7.º da Carta garante o direito ao respeito da vida privada, ao passo que o seu artigo 8.º proclama expressamente o direito à proteção dos dados pessoais. Os n.os 2 e 3 deste último artigo precisam que esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei, que todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação e que o cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

A - Quanto às competências das autoridades nacionais de controlo em caso de decisão de adequação da Comissão

53. Como M. Schrems refere nas suas observações, para efeitos da queixa no processo principal, a questão central é a da transferência de dados pessoais da Facebook Ireland para a Facebook USA à luz do acesso generalizado da NSA e de outras agências de segurança americanas dos Estados Unidos aos dados armazenados na Facebook USA ao abrigo das competências que lhes confere a legislação americana.

54. Segundo M. Schrems, na sequência de uma queixa que pretende pôr em causa a constatação de que um país terceiro assegura um nível de proteção adequado aos dados transferidos, a autoridade nacional de controlo pode, se dispuser de elementos no sentido da procedência das alegações contidas nessa queixa, ordenar a suspensão da transferência de dados operada pela empresa designada na referida queixa.

55. Tendo em conta a obrigação do Comissário proteger os direitos fundamentais de M. Schrems, este último sustenta que o Comissário tem não só a obrigação de investigar, mas também, se a queixa merecer acolhimento, de utilizar as suas competências para suspender o fluxo de dados entre a Facebook Ireland e a Facebook USA.

56. Ora, o Comissário rejeitou a queixa com base em disposições da Lei sobre a proteção de dados que enumeram os seus poderes. Esta conclusão baseava-se no seu entendimento de que estava vinculado pela Decisão 2000/520.

57. Daqui decorre que o problema central no presente processo é o de saber se, a apreciação da Comissão quanto à adequação do nível de proteção contida na Decisão 2000/520 vincula absolutamente a autoridade nacional para a proteção de dados e a impede de investigar as alegações que pretendem pôr em causa essa constatação. Por conseguinte, as questões prejudiciais têm por objeto o alcance dos poderes de investigação das autoridades nacionais para a proteção de dados perante uma decisão de adequação da Comissão.

58. Segundo a Comissão há que ter em conta a articulação entre os seus respetivos poderes e os das autoridades nacionais para a proteção de dados. As competências destas últimas centram-se na aplicação da legislação nessa matéria aos casos individuais, ao passo que o reexame geral da aplicação da Decisão 2000/520, incluindo-se aí qualquer decisão que envolva a sua suspensão ou a sua revogação, se enquadra na competência da Comissão.

59. A Comissão alega que M. Schrems não apresentou argumentos específicos que fizessem pensar que corria um risco iminente de sofrer danos graves em consequência da transferência de dados entre a Facebook Ireland e a Facebook USA. Pelo contrário, por causa da sua natureza geral e abstrata, as preocupações expressas por M. Schrems a propósito dos programas de vigilância implementado pelas agências de segurança americanas eram idênticas às que levaram a Comissão a proceder à revisão da Decisão 2000/520.

60. Segundo a Comissão, as autoridades nacionais de controlo interfeririam com as competências de que dispõe para renegociar as condições dessa decisão com os Estados Unidos ou, se necessário, para a suspender, se adotassem medidas com base em queixas que apenas dão conta de preocupações estruturais e abstratas.

61. Não partilho da opinião da Comissão. No meu entendimento, a existência de uma decisão aprovada pela Comissão com fundamento no artigo 25.º, n.º 6, da Diretiva 95/46 não pode anular ou mesmo reduzir os poderes de que dispõem as autoridades nacionais de controlo nos termos do artigo 28.º desta diretiva. Contrariamente ao que a Comissão alega, embora as autoridades nacionais de controlo sejam chamadas a pronunciar-se no âmbito de queixas individuais, isso não as impede, no seu entender, ao abrigo dos seus poderes de investigação e da sua independência, de formarem a sua própria opinião sobre o nível geral de proteção assegurada por um país terceiro e de daí tirar as consequências quando decidem sobre casos individuais.

62. Decorre de jurisprudência constante do Tribunal de Justiça que, para a interpretação de disposições de direito da União, há que ter em conta não só os seus termos mas também o seu contexto e os objetivos prosseguidos pela regulamentação de que fazem parte [22].

63. Resulta do considerando 62 da Diretiva 95/46 que «a criação, nos Estados-Membros, de autoridades de controlo que exerçam as suas funções com total independência constitui um elemento essencial da proteção das pessoas no que respeita ao tratamento de dados pessoais».

64. Nos termos do artigo 28.º, n.º 1, primeiro parágrafo, desta diretiva, «[c]ada Estado-Membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adotadas pelos Estados-Membros nos termos da presente diretiva». O artigo 28.º, n.º 1, segundo parágrafo dispõe que «[e]ssas autoridades exercerão com total independência as funções que lhes forem atribuídas».

65. O artigo 28.º, n.º 3, da Diretiva 95/46 enumera os poderes que cada autoridade de controlo dispõe, a saber, poderes de inquérito, poderes efetivos de intervenção que lhe permitem, designadamente, proibir temporária ou definitivamente um tratamento, e o poder de intervir em processos judiciais no caso de violações das disposições nacionais adotadas nos termos da presente diretiva ou de levar essas infrações ao conhecimento das autoridades judiciais.

66. Por outro lado, nos termos do artigo 28.º, n.º 4, primeiro parágrafo, da Diretiva 95/46, «[q]ualquer pessoa [...] pode apresentar à autoridade de controlo um pedido para proteção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais». O artigo 28.º, n.º 4, segundo parágrafo, desta diretiva esclarece que «[e]m particular, qualquer pessoa pode apresentar à autoridade de controlo um pedido de verificação da licitude de qualquer tratamento de dados, sempre que sejam aplicáveis as disposições nacionais adotadas por força do artigo 13.º». Preciso que esta última disposição permite aos Estados-Membros adotar medidas legislativas que visem limitar o alcance de diversas obrigações e direitos previstos na Diretiva 95/46, quando essa limitação constitua uma medida necessária para salvaguardar, nomeadamente, a segurança do Estado, a defesa, a segurança pública, bem como a prevenção, a investigação, a deteção e a repressão de infrações penais.

67. Conforme o Tribunal de Justiça já salientou, a exigência de fiscalização, por uma autoridade independente, do cumprimento das regras da União relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais resulta também do direito primário da União, nomeadamente do artigo 8.º, n.º 3, da Carta e do artigo 16.º, n.º 2, TFUE [23]. O Tribunal recordou também que «[a]instituição, nos Estados-Membros, de autoridades de fiscalização independentes constitui, pois, um elemento essencial da proteção das pessoas no que diz respeito ao tratamento de dados pessoais» [24].

68. O Tribunal de Justiça já declarou também que «o artigo 28.º, n.º 1, segundo parágrafo, da Diretiva 95/46 deve ser interpretado no sentido de que as autoridades de controlo competentes para a supervisão do tratamento de dados pessoais devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. Esta independência exclui, designadamente, qualquer instrução e qualquer outra influência externa, sob qualquer forma, seja direta ou indireta, suscetíveis de orientar as suas decisões e que podem assim pôr em causa o cumprimento, pelas referidas autoridades, da sua função de estabelecer um justo equilíbrio entre a proteção do direito à vida privada e a livre circulação dos dados de natureza pessoal» [25].

22 — V., nomeadamente, acórdão Koushkaki (C-84/12, EU:C:2013:862, n.º 34 e jurisprudência referida).

23 — V. acórdãos Comissão/Áustria (C-614/10, EU:C:2012:631, n.º 36) e Comissão/Hungria (C-288/12, EU:C:2014:237, n.º 47).

24 — V., nomeadamente, acórdãos, Comissão/Hungria (C-288/12, EU:C:2014:237, n.º 48 e jurisprudência referida). V., também, neste sentido, acórdão Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238, n.º 68 e jurisprudência referida).

25 — V., nomeadamente, acórdão Comissão/Hungria (C-288/12, EU:C:2014:237, n.º 51 e jurisprudência referida).

69. O Tribunal de Justiça precisou também que «[a] garantia de independência das autoridades nacionais da fiscalização visa assegurar a eficácia e a fiabilidade da fiscalização do respeito das disposições em matéria de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais» [26]. Esta garantia de independência foi estabelecida «com vista a reforçar a proteção das pessoas e dos organismos abrangidos pelas [...] decisões [dessas autoridades nacionais de controlo]» [27].

70. Como resulta nomeadamente do considerando 10 e do artigo 1.º da Diretiva 95/46, esta procura garantir no seio da União, «um nível elevado de proteção das liberdades e dos direitos fundamentais no que diz respeito ao tratamento de dados pessoais» [28]. Segundo o Tribunal de Justiça, «[a]s autoridades de controlo previstas no artigo 28.º da Diretiva 95/46 são, portanto, as guardiãs dos referidos direitos e liberdades fundamentais» [29].

71. Tendo em conta a importância do papel desempenhado pelas autoridades nacionais de controlo em matéria de proteção das pessoas singulares relativamente ao tratamento de dados pessoais, os seus poderes de intervenção devem manter-se plenamente mesmo quando a Comissão adotou uma decisão com fundamento no artigo 25.º, n.º 6 da Diretiva 95/46.

72. A este respeito, observo que não há nada que indique que os sistemas de transferência de dados pessoais para países terceiros estejam excluídos do âmbito de aplicação material do artigo 8.º, n.º 3, da Carta, que consagra ao mais alto nível da hierarquia das normas em direito da União a importância da fiscalização exercida por uma autoridade independente no que se refere ao respeito das regras relativas à proteção de dados pessoais.

73. Se as autoridades nacionais de controlo estivessem absolutamente vinculadas pelas decisões adotadas pela Comissão, isso limitaria inevitavelmente a sua total independência. Em conformidade com o seu papel de guardiãs dos direitos fundamentais, as autoridades nacionais de controlo devem poder investigar, com toda a independência, as reclamações que lhes sejam apresentadas, no superior interesse da proteção das pessoas relativamente ao tratamento de dados pessoais.

74. Além disso, como realçaram com razão o Governo belga e o Parlamento Europeu na audiência, não há nenhuma relação de hierarquia entre o capítulo IV da Diretiva 95/46 relativo à transferência de dados pessoais para países terceiros e o seu capítulo VI consagrado, nomeadamente, ao papel das autoridades nacionais de controlo. Não há nada no capítulo VI que sugira que as disposições relativas às autoridades nacionais de controlo estejam subordinadas de uma qualquer maneira às disposições distintas sobre as transferências enunciadas no capítulo IV da Diretiva 95/46.

75. Pelo contrário, resulta expressamente do artigo 25.º, n.º 1, que se insere no capítulo IV, desta diretiva, que a autorização de transferência de dados pessoais para um país terceiro que assegura um nível de proteção adequado, só pode realizar-se, sob reserva da observância das disposições nacionais adotadas nos termos das outras disposições da referida diretiva.

76. A este propósito, recordo que, por força desta disposição, os Estados-Membros devem prever na respetiva legislação nacional que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se, sob reserva da observância das disposições nacionais adotadas nos termos das outras disposições da Diretiva 95/46, se o país terceiro em questão assegurar um nível de proteção adequado.

26 — Acórdão Comissão/Alemanha (C-518/07, EU:C:2010:125, n.º 25).

27 — *Idem.*

28 — *Ibidem* (n.º 22 e jurisprudência referida).

29 — *Ibidem* (n.º 23). V., também, neste sentido, acórdãos Comissão/Áustria (C-614/10, EU:C:2012:631, n.º 52), e Comissão/Hungria (C-288/12, EU:C:2014:237, n.º 53).

77. Em conformidade com o artigo 28.º, n.º 1, desta diretiva, as autoridades nacionais de controlo são responsáveis pela fiscalização da aplicação no território de cada Estado-Membro, das disposições adotadas pelos Estados-Membros nos termos da referida diretiva.

78. A aproximação entre estas duas disposições permite considerar que a regra enunciada no artigo 25.º, n.º 1, da Diretiva 95/46, nos termos da qual a transferência de dados pessoais só pode realizar-se se o país terceiro destinatário lhes assegurar um nível de proteção adequado, faz parte das regras cuja aplicação as autoridades nacionais de controlo devem fiscalizar.

79. Importa interpretar em sentido amplo, em conformidade com o artigo 8.º, n.º 3, da Carta, os poderes das autoridades nacionais de controlo para investigar com toda a independência as reclamações que lhes forem apresentadas, nos termos do artigo 28.º da Diretiva 95/46. Por conseguinte, esses poderes não podem ser limitados pelos poderes conferidos pelo legislador da União à Comissão, nos termos do artigo 25.º, n.º 6, desta diretiva, para constatar o caráter adequado do nível de proteção oferecido por um país terceiro.

80. Tendo em conta o seu papel essencial em matéria de proteção de dados pessoais, as autoridades nacionais de controlo devem poder investigar quando lhes é apresentada uma queixa que dá a conhecer factos que podem ser suscetíveis de pôr em causa o nível de proteção assegurado por um país terceiro, incluindo quando a Comissão constatou, numa decisão adotada com fundamento no artigo 25.º, n.º 6, da Diretiva 95/46, que o país terceiro em questão assegura um nível de proteção adequado.

81. Se, no termo das investigações conduzidas por uma autoridade nacional de controlo, esta considerar que a transferência de dados contestada prejudica a proteção de que devem beneficiar os cidadãos da União quanto ao tratamento dos seus dados, tem o poder de suspender a transferência de dados em causa, e isto, independentemente da avaliação geral feita pela Comissão na sua decisão.

82. Com efeito, é pacífico, nos termos do artigo 25.º, n.º 2, da Diretiva 95/46, que a adequação do nível de proteção oferecido por um país terceiro é apreciada em função de um conjunto de circunstâncias tanto factuais como jurídicas. Se uma dessas circunstâncias evoluir e revelar ser suscetível de pôr em causa a adequação do nível de proteção oferecido por um país terceiro, a autoridade nacional de controlo à qual a queixa foi submetida deve poder tirar daí as consequências em relação à transferência contestada.

83. É certo que, como a Irlanda salientou, o Comissário, como as outras autoridades estatais, está vinculado pela Decisão 2000/520. Com efeito, resulta do artigo 288.º, quarto parágrafo, TFUE que uma decisão aprovada por uma instituição da União é obrigatória em todos os seus elementos. Consequentemente, a Decisão 2000/520 impõe-se aos Estados-Membros a que é destinada.

84. A este respeito, saliento que a própria Decisão 2000/520 dispõe, no seu artigo 5.º, que «[o]s Estados-Membros tomarão todas as medidas necessárias para [lhe] dar cumprimento, o mais tardar até 90 dias após a data da sua notificação aos Estados-Membros». Além disso, o artigo 6.º desta decisão confirma que «[o]s Estados-Membros são os destinatários [desta]».

85. No entanto, considero que, tendo em conta as disposições *supra* referidas da Diretiva 95/46 e da Carta, o efeito obrigatório da Decisão 2000/520 não é suscetível de excluir qualquer investigação do Comissário sobre queixas que aleguem que transferências de dados pessoais efetuadas para os Estados Unidos no âmbito desta decisão não apresentam as garantias necessárias de proteção requeridas pelo direito da União. Por outras palavras, esse efeito vinculativo não é suscetível de impor que qualquer queixa desse género que seja rejeitada sumariamente, isto é, imediatamente e sem nenhuma análise da sua justeza.

86. Acrescento, além disso, que resulta da economia do artigo 25.º da Diretiva 95/46 que a constatação de que um país terceiro assegura ou não um nível de proteção adequado pode ser feita quer pelos Estados-Membros, quer pela Comissão. Por conseguinte, trata-se de uma competência partilhada.

87. Resulta do artigo 25.º, n.º 6, desta diretiva que, quando a Comissão constata que um país terceiro assegura um nível de proteção adequado na aceção do artigo 25.º, n.º 2, da referida diretiva, os Estados-Membros devem tomar as medidas necessárias para dar cumprimento à decisão da Comissão.

88. Uma vez que essa decisão tem o efeito de permitir as transferências de dados pessoais para um país terceiro cujo nível de proteção a Comissão considera adequado, os Estados-Membros devem, consequentemente, permitir, em princípio, que essas transferências sejam efetuadas pelas empresas estabelecidas no respetivo território.

89. No entanto, o artigo 25.º da Diretiva 95/46 não atribui à Comissão a exclusividade em matéria de constatação do nível adequado ou não da proteção dos dados pessoais transferidos. A economia deste artigo demonstra que os Estados-Membros ocupam também um papel na matéria. Uma decisão da Comissão desempenha, é certo, um papel importante na uniformização das condições de transferência válidas nos Estados-Membros. No entanto, essa uniformização só pode perdurar enquanto a constatação não for posta em causa.

90. O argumento da necessária uniformização das condições de transferência de dados pessoais para um país terceiro encontra, na minha opinião, o seu limite numa situação como a que está em causa no processo principal onde não só a Comissão é informada de que a sua constatação está sujeita a críticas, mas também em que é ela própria que formula tais críticas e enceta reuniões para as sanar.

91. A avaliação do caráter adequado ou não do nível da proteção oferecido por um país terceiro pode também dar lugar a uma cooperação entre os Estados-Membros e a Comissão. A este propósito, o artigo 25.º, n.º 3, da Diretiva 95/46 prevê que «[o]s Estados-Membros e a Comissão informar-se-ão mutuamente dos casos em que consideram que um país terceiro não assegura um nível de proteção adequado na aceção do n.º 2». Conforme observa o Parlamento, isso demonstra que os Estados-Membros e a Comissão têm um papel equivalente a desempenhar para assinalar as situações em que um país terceiro não assegura um nível de proteção adequado.

92. A decisão de adequação tem o objetivo de autorizar a transferência de dados pessoais para o país terceiro em causa. Isso não implica que os cidadãos da União tenham deixado de poder apresentar pedidos às autoridades de controlo com vista à proteção dos seus dados pessoais. Observo, a este propósito, que o artigo 28.º, n.º 4, primeiro parágrafo, da Diretiva 95/46, segundo o qual «[q]ualquer pessoa [...] pode apresentar à autoridade de controlo um pedido para proteção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais», não prevê exceção a este princípio no caso de existir uma decisão adotada pela Comissão nos termos do artigo 25.º, n.º 6, desta diretiva.

93. Assim, embora uma decisão adotada pela Comissão no exercício dos poderes de execução que lhe são conferidos por esta última disposição tenha o efeito de permitir a transferência de dados pessoais para um país terceiro, uma decisão dessa natureza não pode, em contrapartida, ter o efeito de retirar todo o poder aos Estados-Membros, e, em especial às suas autoridades nacionais de controlo, ou mesmo restringir apenas as suas competências, quando confrontados com alegações de violação de direitos fundamentais.

94. Uma autoridade nacional de controlo deve estar em condições de exercer os poderes previstos no artigo 28.º, n.º 3, da Diretiva 95/46, nomeadamente o de proibir temporária ou definitivamente o tratamento de dados pessoais. Embora a enumeração dos poderes, prevista nesta disposição, não preveja explicitamente poderes relativos a uma transferência de um Estado-Membro para um país

terceiro, essa transferência deve, na minha opinião, ser considerada um tratamento de dados [30]. Além disso, como resulta da redação da referida disposição, a enumeração não é exaustiva. Em todo o caso, tendo em conta o papel essencial desempenhado pelas autoridades nacionais de controlo no sistema instituído pela Diretiva 95/46, estas devem dispor do poder de suspender uma transferência de dados em caso de dano comprovado ou de risco de dano aos direitos fundamentais.

95. Acrescento que privar a autoridade nacional de controlo dos seus poderes de investigação em circunstâncias como as que estão em causa no presente processo seria contrário não só ao princípio de independência, mas também ao objetivo da Diretiva 95/46 conforme resulta do seu artigo 1.º, n.º 1.

96. Como o Tribunal de Justiça salientou, [r]esulta dos considerandos 3, 8 e 10 da Diretiva 95/46 que o legislador da União pretendeu facilitar a livre circulação de dados pessoais através da aproximação das legislações dos Estados-Membros, embora salvaguardando os direitos fundamentais das pessoas, nomeadamente o direito à proteção da vida privada, e garantindo um nível elevado de proteção na União. O artigo 1.º desta diretiva prevê assim que os Estados-Membros devem assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do seu direito à vida privada, no que diz respeito ao tratamento de dados pessoais» [31].

97. Por conseguinte, as disposições da Diretiva 95/46 devem ser interpretadas em conformidade com o seu objetivo que visa garantir um nível elevado de proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente a sua vida privada, tendo em conta o tratamento dos dados pessoais na União.

98. A importância deste objetivo e o papel que os Estados-Membros devem desempenhar para o atingir implicam que, quando circunstâncias específicas geram uma dúvida séria quanto ao respeito dos direitos fundamentais garantidos pela Carta em caso de transferência de dados pessoais para um país terceiro, os Estados-Membros e, consequentemente, as respetivas autoridades nacionais de controlo não podem estar vinculados em termos absolutos por uma decisão de adequação da Comissão.

99. O Tribunal de Justiça já declarou que «as disposições da Diretiva 95/46, na medida em que regulam o tratamento de dados pessoais suscetíveis de pôr em causa as liberdades fundamentais e, em especial, o direito à vida privada, devem necessariamente ser interpretadas à luz dos direitos fundamentais que, segundo jurisprudência constante, são parte integrante dos princípios gerais de direito cujo respeito é assegurado pelo Tribunal de Justiça e que estão atualmente consagrados na Carta» [32].

100. Além disso, refiro-me à jurisprudência segundo a qual «compete aos Estados-Membros não só interpretar o seu direito nacional em conformidade com o direito da União, mas também velar por que não se tome por base uma interpretação de um diploma de direito derivado que seja suscetível de entrar em conflito com os direitos fundamentais protegidos pela ordem jurídica da União ou com os outros princípios gerais do direito da União» [33].

30 — V. conclusões do advogado-geral P. Léger apresentadas no processo Parlamento/Conselho e Comissão (C-317/04, EU:C:2005:710, n.os 92 a 95). V., também, acórdão Parlamento/Conselho e Comissão (C-317/04 e C-318/04, EU:C:2006:346, n.º 56).

31 — V., nomeadamente, acórdão IPI (C-473/12, EU:C:2013:715, n.º 28 e jurisprudência referida).

32 — V., nomeadamente, acórdão Google Spain e Google (C-131/12, EU:C:2014:317, n.º 68 e jurisprudência referida).

33 — V., nomeadamente, acórdão N. S. e o. (C-411/10 e C-493/10, EU:C:2011:865, n.º 77 e jurisprudência referida).

101. O Tribunal de Justiça também declarou, no seu acórdão N. S. e o.[34], que «uma aplicação do Regulamento [(CE)] n.º 343/2003 [[35]] com base na presunção inilidível de que os direitos fundamentais do requerente de asilo são respeitados no Estado-Membro normalmente competente para conhecer o seu pedido é incompatível com a obrigação de os Estados-Membros interpretarem e aplicarem o Regulamento n.º 343/2003 em conformidade com os direitos fundamentais»[36].

102. A este propósito, o Tribunal de Justiça reconheceu, no âmbito do estatuto que os Estados-Membros enquanto países de origem seguros têm para com os outros para as questões jurídicas e práticas relacionadas com o direito de asilo, que se deve presumir que o tratamento dado aos requerentes de asilo em cada Estado-Membro é conforme com as exigências da Carta, da Convenção Relativa ao Estatuto dos Refugiados, assinada em Genebra, em 28 de julho de 1951[37], e da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, assinada em Roma, em 4 de novembro de 1950[38]. No entanto, o Tribunal de Justiça declarou que «[...] não se pode excluir que este sistema se depare, na prática, com grandes dificuldades de funcionamento num determinado Estado-Membro, de modo que existe um sério risco de os requerentes de asilo serem, em caso de transferência para esse Estado-Membro, tratados de modo incompatível com os seus direitos fundamentais»[39].

103. Consequentemente, o Tribunal de Justiça declarou que «incumbe aos Estados-Membros, incluindo os órgãos jurisdicionais nacionais, não transferir um requerente de asilo para o 'Estado-Membro responsável', na aceção do Regulamento n.º 343/2003, quando não possam ignorar que as falhas sistémicas do procedimento de asilo e das condições de acolhimento dos requerentes de asilo nesse Estado-Membro constituem razões sérias e verosímeis de que o requerente corre um risco real de ser sujeito a tratos desumanos ou degradantes, na aceção do artigo 4.º da Carta»[40].

104. Não me parece que o contributo do acórdão N. S. e o.[41] possa ser alargado a uma situação como a que está em causa no processo principal. Assim, uma interpretação do direito derivado da União que assenta numa presunção inilidível de que os direitos fundamentais são respeitados - seja por um Estado-Membro, pela Comissão ou por um país terceiro - deve ser considerada incompatível com a obrigação dos Estados-Membros interpretarem e aplicarem o direito derivado da União de uma maneira conforme com os direitos fundamentais. Por conseguinte, o artigo 25.º, n.º 6, da Diretiva 95/46 não impõe essa presunção inilidível de respeito dos direitos fundamentais relativamente à apreciação pela Comissão do caráter adequado do nível de proteção oferecido por um país terceiro. Pelo contrário, deve-se considerar ilidível a presunção, subjacente a esta disposição, de que a transferência de dados para um país terceiro respeita os direitos fundamentais[42]. Por conseguinte, a referida disposição não deve ser interpretada no sentido de que põe em causa as garantias que figuram nomeadamente no artigo 28.º, n.º 3, da Diretiva 95/46 e no artigo 8.º, n.º 3, da Carta, que visam a proteção e o respeito do direito à proteção dos dados pessoais.

105. Consequentemente, deduzo do referido acórdão que, em caso de falhas sistémicas constatadas no país terceiro para o qual são transferidos os dados pessoais, os Estados-Membros devem poder adotar as medidas necessárias para a salvaguarda dos direitos fundamentais protegidos pelos artigos 7.° e 8.° da Carta.

34 — C-411/10 e C-493/10, EU:C:2011:865.

35 — Regulamento do Conselho, de 18 de fevereiro de 2003, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de asilo apresentado num dos Estados-Membros por um nacional de um país terceiro (JO L 50, p. 1).

36 — N.º 99 desse acórdão.

37 — *Recueil des traités des Nations unies*, vol. 189, p. 150, n.º 2545 (1954).

38 — V. acórdão N. S. e o. (C-411/10 e C-493/10, EU:C:2011:865, n.º 80).

39 — *Ibidem* (n.º 81).

40 — *Ibidem* (n.º 94).

41 — C-411/10 e C-493/10, EU:C:2011:865.

42 — N.º 107 deste acórdão.

106. Por outro lado, conforme o Governo italiano salientou nas suas observações, a adoção de uma decisão de adequação pela Comissão não pode ter o efeito de reduzir a proteção dos cidadãos da União relativamente ao tratamento dos seus dados quando estes são transferidos para um país terceiro, por comparação com o nível de proteção de que essas pessoas gozariam se os seus dados fossem tratados na União. Consequentemente, as autoridades nacionais de controlo devem estar em condições de intervir e de exercer os seus poderes em relação à transferência de dados para um país terceiro objeto de uma decisão de adequação. Caso contrário, os cidadãos da União estariam menos bem protegidos do que em caso de tratamento dos seus dados na União.

107. Assim, a adoção de uma decisão pela Comissão nos termos do artigo 25.º, n.º 6, da Diretiva 95/46 só tem o efeito de levantar a proibição geral de exportação dos dados pessoais para países terceiros que garantem um nível de proteção comparável com o que esta diretiva oferece. Por outras palavras, não se trata de criar um regime especial de exceção e menos protetor para os cidadãos da União por comparação com o regime geral previsto pela referida diretiva para os tratamentos de dados que ocorrem na União.

108. É certo que, o Tribunal de Justiça declarou, no n.º 63 do seu acórdão Lindqvist [43], que «[o] capítulo IV da Diretiva 95/46, no qual se insere o artigo 25.º, institui um regime especial». Todavia, na minha opinião, isso não significa que esse regime deva ser menos protetor. Pelo contrário, para atingir o objetivo de proteção de dados fixado no artigo 1.º, n.º 1, da Diretiva 95/46, o seu artigo 25.º impõe uma série de obrigações aos Estados-Membros e à Comissão [44] e este artigo estabelece o princípio segundo o qual sempre que um país terceiro não ofereça um nível de proteção adequado, a transferência de dados de caráter pessoal para esse país deve ser proibida [45].

109. Especificamente, em relação ao sistema «porto seguro», a Comissão só encara a intervenção das autoridades nacionais de controlo e a suspensão por elas dos fluxos de dados no quadro traçado pelo artigo 3.º, n.º 1, alínea b), da Decisão 2000/520.

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

111. No âmbito do presente processo, foi especialmente discutida a aplicação do artigo 3.º, n.º 1, alínea b), da referida decisão. Assim, nos termos desta disposição, a suspensão de fluxos de dados pode ser decidida pelas autoridades nacionais de controlo nos casos «[em que] [e]xistem fortes probabilidades para supor que os princípios não estão a ser respeitados. Há indícios de que o mecanismo de aplicação em causa não toma ou não tomará as medidas adequadas na altura necessária para resolver o caso em questão, que a continuação da transferência dos dados pode causar graves prejuízos às pessoas em causa e que as entidades competentes nos Estados-Membros envidaram esforços razoáveis, dadas as circunstâncias, para facultar à organização em causa a informação e oportunidade necessárias para responder».

43 — C-101/01, EU:C:2003:596.

44 — N.º 65.

45 — N.º 64.

112. A referida disposição levanta várias questões que foram objeto de diversas interpretações pelas partes no decurso do presente processo [46]. Sem entrar no detalhe dessas interpretações, daí resulta que aquelas condições enquadram de forma estrita o poder das autoridades nacionais de controlo para suspender fluxos de dados.

113. Ora, contrariamente ao que a Comissão alega, o artigo 3.º, n,.° 1, alínea b), da Decisão 2000/520 deve ser interpretado em conformidade com o objetivo de proteção dos dados pessoais prosseguido pela Diretiva 95/46 e à luz do artigo 8.º da Carta. O imperativo de interpretação conforme com os direitos fundamentais milita a favor de uma interpretação ampla desta disposição.

114. Daqui resulta que as condições previstas no artigo 3.º, n.º 1, alínea b), da Decisão 2000/520 não podem, no meu entendimento, impedir uma autoridade nacional de controlo de exercer, com toda a independência, os poderes de que está investida, por força do artigo 28.º, n.º 1, da Diretiva 95/46.

115. Como referiram, em substância, os Governos belga e austríaco durante a audiência, a saída alternativa que constitui o artigo 3.º, n.º 1, alínea b), da Decisão 2000/520 é tão estreita que é difícil de pôr em prática. Exige critérios cumulativos e coloca a fasquia demasiado alta. Ora, à luz do artigo 8.º, n.º 3, da Carta, é impossível que a margem de manobra das autoridades nacionais de controlo relativamente às prerrogativas com origem no artigo 28.º, n.º 3, da Diretiva 95/46 seja de tal forma limitada que estas não possam ser exercidas.

116. A este respeito, o Parlamento observou, com razão, que foi o legislador da União, que decidiu quais eram os poderes que deviam incumbir às autoridades nacionais de controlo. Ora, o poder de execução confiado pelo legislador da União à Comissão no artigo 25.º, n.º 6, da Diretiva 95/46 não afeta os poderes conferidos por este mesmo legislador às autoridades nacionais de controlo no artigo 28.º, n.º 3, desta diretiva. Por outras palavras, a Comissão não dispõe da competência de restringir os poderes das autoridades nacionais de controlo.

117. Por conseguinte, para assegurar uma proteção adequada dos direitos fundamentais das pessoas singulares relativamente ao tratamento dos dados pessoais, as autoridades nacionais de controlo devem estar habilitadas a conduzir inquéritos, em caso de alegações que deem conta de violações desses direitos. Se, no termo dessas investigações, estas autoridades considerarem que há num país terceiro abrangido por uma decisão de adequação, indícios sérios de dano ao direito dos cidadãos da União à proteção dos seus dados pessoais, devem poder suspender a transferência de dados para o destinatário estabelecido nesse país terceiro.

118. Por outras palavras, as autoridades nacionais de controlo devem poder conduzir as suas investigações e, sendo caso disso, suspender uma transferência de dados, independentemente das condições restritivas fixadas no artigo 3.º, n.º 1, alínea b), da Decisão 2000/520.

119. Por outro lado, ao abrigo do poder de intervir em processos judiciais no caso de violação das disposições nacionais adotadas nos termos da Diretiva 95/96 ou do seu poder de levar essas infrações ao conhecimento das autoridades judiciais, previstos no artigo 28.º, n.º 3, desta diretiva, as autoridades nacionais de controlo deviam poder, quando têm conhecimento de factos que demonstram que um país terceiro não assegura um nível de proteção adequado, intentar uma ação junto de um tribunal nacional que, pode, se for caso disso, decidir submeter um pedido de decisão prejudicial ao Tribunal de Justiça para apreciar a validade de uma decisão de adequação da Comissão.

46 — Segundo M. Schrems, a primeira condição segundo a qual «[e]xistem fortes probabilidades para supor que os princípios não estão a ser respeitados», não está preenchida. Ora, não é alegado que a Facebook USA, enquanto organismo autocertificado, para o qual os dados são transferidos, tinha ela própria violado os princípios de porto de seguro, devido ao acesso em larga escala e indiferenciado pelas autoridades americanas aos dados que detém. Com efeito, os princípios de porto seguro são expressamente limitados pelo direito americano que o anexo I, quarto parágrafo, da decisão 2000/520 define remetendo para a legislação, para os regulamentos governamentais e para a jurisprudência.

120. Resulta do conjunto destes elementos que o artigo 28.º da Diretiva 95/46, lido à luz dos artigos 7.° e 8.° da Carta, deve ser interpretado no sentido de que a existência de uma decisão adotada pela Comissão com fundamento no artigo 25.º, n.º 6, desta diretiva, não tem o efeito de impedir uma autoridade nacional de controlo de investigar uma queixa que dá a conhecer que um país terceiro não assegura um nível de proteção adequado aos dados pessoais transferidos e, se for caso disso, suspender a transferência desses dados.

121. Embora a High Court sublinhe, na sua decisão de reenvio, que M. Schrems não contestou formalmente no recurso interposto no processo principal nem a validade da Diretiva 95/46 nem da Decisão 2000/520, resulta dessa decisão de reenvio que a crítica principal formulada por M. Schrems visa pôr em causa a constatação de que os Estados Unidos asseguram, no âmbito do sistema «porto seguro», um nível de proteção adequado aos dados pessoais transferidos.

122. Resulta também das observações do Comissário que a queixa de M. Schrems visa pôr diretamente em causa a Decisão 2000/520. Ao apresentar esta queixa, este último quis atacar os termos e o funcionamento do sistema «porto seguro» enquanto tal, pelo facto de a vigilância em larga escala dos dados pessoais para transferidos para os Estados Unidos demonstrar que não existia uma verdadeira proteção desses dados ao nível do direito e das práticas em vigor nesse país terceiro.

123. Além disso, o próprio órgão jurisdicional de reenvio observa que a garantia conferida pelo artigo 7.º da Carta e pelos valores essenciais comuns às tradições constitucionais dos Estados-Membros ficaria comprometida se se permitisse que os poderes públicos acedessem de forma aleatória e generalizada às comunicações eletrónicas sem terem de apresentar uma justificação objetiva baseada em considerações de segurança nacional ou de prevenção da criminalidade ligadas especialmente a determinados indivíduos e sem nenhuma garantia adequada e verificável [47]. O órgão jurisdicional de reenvio suscita assim, indiretamente, dúvidas sobre a validade da Decisão 2000/520.

124. Por conseguinte, a apreciação da questão de saber se os Estados Unidos, no âmbito do sistema «porto seguro» garantem um nível de proteção adequado aos dados pessoais transferidos leva-nos necessariamente a examinar validade desta decisão.

125. A este propósito, importa salientar que, no âmbito do instrumento de cooperação entre o Tribunal de Justiça e os órgãos jurisdicionais nacionais instituído pelo artigo 267.º TFUE, o Tribunal de Justiça, mesmo quando lhe é exclusivamente submetida uma questão prejudicial sobre a interpretação do direito da União, pode, em determinadas circunstâncias específicas, ser levado a analisar a validade de disposições de direito derivado.

126. Por conseguinte, o Tribunal de Justiça declarou por diversas vezes, a título oficioso, a invalidade de um ato quando apenas lhe era pedida a sua interpretação [48]. O Tribunal declarou também que «quando é evidente que o verdadeiro objeto das questões submetidas por um órgão jurisdicional nacional é mais o exame da validade do que a interpretação de atos [da União], compete ao Tribunal de Justiça esclarecer imediatamente esse órgão jurisdicional, sem o obrigar a um formalismo puramente dilatório, incompatível com a própria natureza dos mecanismos instituídos pelo artigo [267.° TFUE]» [49]. Por outro lado, o Tribunal de Justiça já considerou que as dúvidas manifestadas por um órgão jurisdicional nacional sobre a compatibilidade de um ato de direito derivado com as regras relativas à proteção dos direitos fundamentais deviam ser interpretadas no sentido de que põem em causa a validade desse ato à luz do direito da União [50].

47 — N.º 24 da decisão de reenvio.

48 — V., nomeadamente, acórdãos Strehl (62/76, EU:C:1977:18, n.ºs 10 a 17); Roquette Frères (145/79, EU:C:1980:234, n.º 6), e Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, n.ºs 32 a 39).

49 — Acórdão Schwarze (16/65, EU:C:1965:117, p. 1094).

50 — V. acórdão Hauer (44/79, EU:C:1979:290, n.º 16).

127. Recordo que também resulta da jurisprudência do Tribunal de Justiça que os atos das instituições, dos órgãos e dos organismos da União gozam de uma presunção de validade que implica que produzem efeitos jurídicos enquanto não forem revogados, anulados no quadro de um recurso de anulação ou declarados inválidos na sequência de um pedido prejudicial ou de uma questão prévia de ilegalidade. O Tribunal de Justiça tem competência exclusiva para declarar a invalidade de um ato da União, competência que tem por objeto garantir a segurança jurídica ao assegurar a aplicação uniforme do direito da União. Na falta de declaração de invalidade, de modificação ou de revogação pela Comissão, a decisão mantém-se obrigatória em todos os seus elementos e diretamente aplicável em qualquer Estado-Membro [51].

128. Por conseguinte, para dar uma resposta completa ao órgão jurisdicional de reenvio e eliminar as dúvidas expressas ao longo do presente processo sobre a Decisão 2000/520, consideramos que o Tribunal de Justiça devia proceder a uma apreciação da validade desta decisão.

129. Assim sendo, importa também precisar que a análise da questão de saber se a Decisão 2000/520 é ou não válida deve ser circunscrita às alegações que foram objeto de debate no âmbito do presente processo. Com efeito, não foram debatidos neste âmbito todos os aspetos relativos ao funcionamento do sistema «porto seguro», razão pela qual não me parece possível entregarmo-nos aqui a um debate exaustivo das insuficiências do sistema.

130. Em contrapartida, a questão de saber se o acesso generalizado e não limitado dos serviços americanos de informação aos dados transferidos é suscetível de afetar a legalidade da Decisão 2000/520 foi objeto de debate no Tribunal de Justiça, no âmbito do presente processo. Por conseguinte, a validade desta decisão pode ser analisada deste ângulo.

A – *Quanto à validade da Decisão 2000/520*

1. Quanto aos elementos a ter em consideração para analisar a validade da Decisão 2000/520

131. Importa recordar a jurisprudência segundo a qual, «no âmbito de um recurso de anulação, a legalidade do ato deve ser apreciada em função dos elementos de facto e de direito existentes na data de adoção do ato, só podendo a análise da Comissão ser censurada se se mostrar manifestamente errada tendo em conta os elementos de que dispunha no momento da adoção do ato em causa» [52].

132. No seu acórdão Gaz de France — Berliner Investissement [53], o Tribunal de Justiça recordou o princípio segundo o qual «a apreciação da validade de um ato, que compete ao Tribunal de Justiça efetuar no âmbito de um pedido de decisão prejudicial, deve normalmente basear-se na situação que existe no momento da adoção do ato» [54]. No entanto, parece admitir que «a validade de um ato possa, em certos casos, ser apreciada em função de elementos novos verificados posteriormente à sua adoção» [55].

133. Esta abertura assim esboçada pelo Tribunal de Justiça parece-me particularmente pertinente no âmbito do presente processo.

51 — V., nomeadamente, acórdão CIVAD (C-533/10, EU:C:2012:347, n.os 39 a 41 e jurisprudência referida).

52 — V., nomeadamente, acórdão BVGD/Comissão (T-104/07 e T-339/08, EU:T:2013:366, n.º 291), que se refere ao acórdão IECC/Comissão (C-449/98 P, EU:C:2001:275, n.º 87).

53 — C-247/08, EU:C:2009:600.

54 — N.º 49 e jurisprudência referida.

55 — N.º 50 e jurisprudência referida. V., neste sentido, Lenaerts, K., Maselis, I., e Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, que enunciam que, «in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court» (n.º 10.16, p. 471).

134. Com efeito, as decisões adotadas pela Comissão com fundamento no artigo 25.º, n.º 6, da Diretiva 95/46 apresentam características específicas. Destinam-se a avaliar se o nível de proteção dos dados pessoais oferecido por um país terceiro apresenta ou não um caráter adequado. Trata-se aí de uma avaliação que está destinada a evoluir em função do contexto factual e jurídico que prevalece no país terceiro.

135. Tendo em conta o facto de que a decisão de adequação constitui um tipo específico de decisão, a regra segundo a qual a apreciação da sua validade só pode ser feita em função dos elementos que existem na data da sua adoção deve ser flexível neste caso. Uma tal regra levaria a que vários anos depois da adoção de uma decisão de adequação, a apreciação de validade que o Tribunal de Justiça fizesse só pudesse ter em conta eventos que ocorreram ulteriormente, e isto mesmo que um tal reenvio prejudicial para apreciação da validade não tenha limite no tempo e que o seu lançamento possa ser precisamente a consequência de factos posteriores que revelam as insuficiências do ato em causa.

136. No caso em apreço, a manutenção em vigor da Decisão 2000/520 durante cerca de 15 anos testemunha a confirmação implícita da avaliação feita em 2000 pela Comissão. Quando, no âmbito de um pedido de decisão prejudicial, o Tribunal de Justiça é levado a analisar a validade de uma avaliação mantida no tempo pela Comissão, é, portanto, não só possível, mas também adequado que possa confrontar esta avaliação com circunstâncias novas que ocorreram depois da adoção da decisão de adequação.

137. Tendo em conta a natureza específica da decisão de adequação, a Comissão deve reexaminá-la regularmente. Se, na sequência de novos eventos corridos entretanto, a Comissão não altera a sua decisão, é porque confirma implícita, mas necessariamente, a apreciação feita inicialmente. Assim, reitera a sua constatação de que o país terceiro em causa assegura um nível de proteção adequado aos dados pessoais transferidos. Compete ao Tribunal de Justiça verificar se esta constatação continua a ser válida apesar das circunstâncias ocorridas posteriormente.

138. Por conseguinte, para assegurar uma fiscalização jurisdicional efetiva deste tipo de decisão, a apreciação da sua validade deve, na minha opinião, ser efetuada tendo em conta o contexto factual e jurídico atual.

2. Quanto ao conceito de nível de proteção adequado

139. O artigo 25.º da Diretiva 95/46 assenta inteiramente no princípio de que a transferência de dados pessoais para um país terceiro só pode ter lugar se esse país terceiro assegurar um nível de proteção adequado a esses dados. Assim, o objetivo deste artigo é assegurar a continuidade da proteção conferida por esta diretiva em caso de transferência de dados pessoais para um país terceiro. A este propósito, importa recordar que a referida diretiva assegura um nível elevado de proteção dos cidadãos da União relativamente ao tratamento dos seus dados pessoais.

140. Tendo em conta o papel importante que a proteção dos dados pessoais desempenha à luz do direito fundamental do respeito da vida privada, esse nível elevado de proteção deve, portanto, ser garantido inclusive em caso de transferência dos dados pessoais para um país terceiro.

141. É por este motivo que considero que a Comissão só pode constatar, com fundamento no artigo 25.º, n.º 6, da Diretiva 95/46, que um país terceiro assegura um nível de proteção adequado, quando no termo de uma avaliação do direito e da prática no país terceiro em questão, estiver em condições de determinar que esse país terceiro assegura um nível de proteção substancialmente equivalente ao conferido por esta diretiva, mesmo que as modalidades dessa proteção possam ser diferentes das utilizadas geralmente na União.

142. Embora o vocábulo inglês «*adequate*» possa entender-se, de um ponto de vista linguístico, no sentido de que designa exatamente um nível de proteção satisfatório ou suficiente, e ter assim um campo semântico diferente do vocábulo francês «*adéquat*», há que observar que o único critério que deve guiar a interpretação desta palavra é o objetivo de atingir um nível de proteção elevado dos direitos fundamentais, como exige a Diretiva 95/46.

143. A análise do nível de proteção assegurado por um país terceiro deve compreender duas vertentes de base: o conteúdo das regras aplicáveis e os meios destinados a assegurar a sua aplicação eficaz [56].

144. Na minha opinião, para atingir um nível de proteção substancialmente equivalente ao que vigora na União, o sistema «porto seguro», que assenta em grande parte na autocertificação e na autoavaliação pelas empresas que participam voluntariamente neste sistema, deve ser acompanhado de garantias adequadas e de um mecanismo de fiscalização suficiente. Assim, as transferências de dados pessoais para um país terceiro não devem beneficiar de uma proteção inferior aos tratamentos efetuados na União.

145. A este respeito, saliento, antes de mais, que, na União, prevalece a conceção segundo a qual um dispositivo de fiscalização externo sob a forma de uma autoridade independente constitui um elemento necessário de todo o sistema que visa assegurar o respeito das regras relativas à proteção dos dados pessoais.

146. Por outro lado, para assegurar o efeito útil do artigo 25.º, n.ºs 1 a 3, da Diretiva 95/46, há que ter em conta o facto de o caráter adequado do nível de proteção oferecido por um país terceiro ser uma situação evolutiva que pode mudar ao longo do tempo em função de uma série de fatores. Assim, os Estados-Membros e a Comissão devem estar constantemente atentos a qualquer alteração de circunstâncias suscetível de tornar necessária uma reavaliação do caráter adequado do nível de proteção oferecida por um país terceiro. Uma avaliação do caráter adequado do nível dessa proteção nunca pode ser fixada num determinado momento e, depois, mantida indefinidamente, independentemente de qualquer alteração de circunstâncias que revelam que o nível de proteção oferecido já não é adequado.

147. A obrigação de o país terceiro assegurar um nível de proteção adequado constitui assim uma obrigação contínua. Embora a avaliação seja feita em relação a um dado momento, a manutenção da decisão de adequação pressupõe que nenhuma circunstância ocorrida posteriormente seja suscetível de pôr em causa a avaliação inicial feita pela Comissão.

148. Com efeito, não se deve perder de vista que o objetivo do artigo 25.º da Diretiva 95/46 é sempre evitar que os dados pessoais sejam transferidos para um país terceiro que não assegura um nível de proteção adequado, em violação do direito fundamental à proteção dos dados pessoais garantido pelo artigo 8.º da Carta.

149. Importa sublinhar que o poder conferido pelo legislador da União à Comissão, no artigo 25.º, n.º 6, Diretiva 95/46, de constatar que um país terceiro assegura um nível de proteção adequado está expressamente condicionado pela exigência de esse país terceiro assegurar esse nível na aceção do n.º 2 daquele artigo. Se novas circunstâncias forem suscetíveis de pôr em causa a avaliação inicial da Comissão, esta deve adaptar a sua decisão em conformidade.

56 — V. p. 5 do documento de trabalho WP 12 da Comissão, intitulado «Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.° e 26.° da Diretiva relativa à proteção de dados», adotada pelo Grupo de Trabalho de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, em 24 de julho de 1998.

3. Análise

150. Recordo que, nos termos do artigo 25.º, n.º 6, da Diretiva 95/46, «[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». Lido em conjugação com o artigo 25.º, n.º 2, desta diretiva, o seu artigo 25.º, n.º 6 significa que, para constatar que um país terceiro assegura um nível de proteção adequado, a Comissão deve proceder a uma avaliação de conjunto das regras de direito em vigor nesse país terceiro e da sua aplicação.

151. Vimos que a manutenção da Decisão 2000/520 pela Comissão, apesar do surgimento de novos elementos factuais e jurídicos, deve ser entendida como a sua vontade de confirmar a sua avaliação inicial.

152. Não compete ao Tribunal de Justiça, no âmbito de um pedido de decisão prejudicial, apreciar os factos que estão na origem do litígio que levou o órgão jurisdicional nacional a fazer este pedido de reenvio [57].

153. Por conseguinte apoiar-me-ei nos factos indicados pelo órgão jurisdicional de reenvio no seu pedido de decisão prejudicial, factos que, de resto, estão amplamente admitidos como assentes pela própria Comissão [58].

154. Os elementos que foram alegados perante o Tribunal de Justiça, para contestar a avaliação da Comissão segundo a qual o sistema relativo ao porto seguro assegura um nível de proteção adequado aos dados pessoais transferidos a partir da União para os Estados Unidos, podem ser descritos nos seguintes termos.

155. No seu pedido de decisão prejudicial, o órgão jurisdicional de reenvio parte das duas constatações factuais seguintes. Por um lado, os dados pessoais transferidos por empresas como a Facebook Ireland para a sua sociedade-mãe com sede nos Estados Unidos podem, de seguida, ser consultados pela NSA e por outras agências de segurança americanas no decurso de atividades de vigilância e de interceção em larga escala e não dirigidas. Com efeito, na sequência das revelações de E. Snowden, não se pode, presentemente, tirar nenhuma outra conclusão plausível dos elementos de prova disponíveis [59]. Por outro lado, os cidadãos da União não dispõem de nenhum direito efetivo de serem ouvidos sobre a questão da vigilância e da interceção dos seus dados pela NSA e por outras agências de segurança americanas [60].

156. Assim, as constatações factuais da High Court estão suportadas nas constatações feitas pela própria Comissão.

157. Deste modo, na sua Comunicação sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE, *supra* referido, a Comissão partiu da constatação de que, em 2013, as informações sobre a dimensão e o âmbito dos programas de vigilância americanos suscitaram grandes preocupações sobre a continuação da proteção de dados pessoais legalmente transferidos para os Estados Unidos ao abrigo do sistema de «porto seguro».

57 — V., nomeadamente, acórdão Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, n.º 22 e jurisprudência referida).

58 — V. comunicação da Comissão mencionada na nota 2 de pé de página e 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].

59 — N.º 7, alínea c), da decisão de reenvio.

60 — N.º 7, alínea b), da decisão de reenvio.

Salientou que todas as empresas que participam no Programa PRISM, que permite às autoridades americanas ter acesso a dados armazenados e tratados nos EUA, parecem estar certificadas no âmbito do sistema de «porto seguro». Na sua opinião, este sistema passou, pois, a ser uma das vias através da qual os serviços de informações americanos têm acesso à recolha de dados pessoais inicialmente tratados na UE [61].

158. Resulta destes elementos que o direito e a prática dos Estados Unidos permitem recolher, em larga escala, dados pessoais de cidadãos de União que são transferidos no âmbito do sistema «porto seguro», sem que estes beneficiem de uma proteção jurisdicional efetiva.

159. Na minha opinião, estas constatações factuais demonstram que a Decisão 2000/520 não contem garantias suficientes. Devido a esta falta de garantias, esta decisão foi executada de uma maneira que não responde aos requisitos previstos na Carta e na Diretiva 95/46.

160. Ora, uma decisão adotada pela Comissão com fundamento no artigo 25.º, n.º 6, da Diretiva 95/46 tem por objeto constatar que um país terceiro «assegura» um nível de proteção adequado. O vocábulo «assegura», conjugado no presente, implica que, para poder ser mantida, essa decisão deve dizer respeito a um país que continua, depois da aprovação da referida decisão, a garantir um nível de proteção adequado.

161. Na realidade, as revelações que são referidas sobre os comportamentos da NSA que utilizava os dados transferidos no âmbito do sistema «porto seguro» lançaram o alerta sobre as falhas da base legal que constitui a Decisão 2000/520.

162. As insuficiências que foram reveladas no decurso do presente processo figuram especificamente do anexo I, quarto parágrafo, desta decisão.

163. Recordo que nos termos desta disposição, «[a] adesão a estes princípios [de «porto seguro»] pode ser limitada: a) na medida necessária para observar requisitos de segurança nacional, interesse público ou execução legal, b) por legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores avançados por essa autorização».

164. O problema resulta essencialmente da utilização que as autoridades americanas fazem das derrogações previstas nesta disposição. Devido à sua formulação demasiado geral, a execução destas derrogações por estas autoridades não está limitada ao estritamente necessário.

165. A essa formulação demasiado geral, acresce a circunstância de os cidadãos da União não disporem de via de recurso adaptada contra o tratamento dos seus dados pessoais para fins diferentes daqueles para que foram inicialmente coligidos e em seguida transferidos para os Estados Unidos.

166. As derrogações previstas pela Decisão 2000/520 à aplicação dos princípios de «porto seguro», nomeadamente por exigências de segurança nacional, deviam ser acompanhados pela implementação de um mecanismo de controlo independente capaz de evitar as violações constatadas ao direito à vida privada.

167. Assim, as revelações sobre as práticas dos serviços de informação americanos quanto à vigilância generalizada dos dados transferidos no âmbito de «porto seguro» lançaram o alerta sobre diversas falhas da Decisão 2000/520.

61 — P. 19 da sua comunicação.

168. As alegações feitas no âmbito do presente processo não são constitutivas de uma violação dos princípios de «porto seguro» pela Facebook. Se uma empresa certificada, como a Facebook USA, dá às autoridades americanas acesso aos dados que lhe foram transferidos de um Estado-Membro, pode ser considerado que o faz para se conformar com a legislação americana. Tendo em conta o facto de essa situação ser expressamente admitida pela Decisão 2000/520, em resultado da formulação ampla das derrogações que prevê, na realidade, é a questão da compatibilidade dessas derrogações com o direito primário da União que é suscitada no âmbito do presente processo.

169. A este propósito, cabe sublinhar que resulta de jurisprudência constante do Tribunal de Justiça que o respeito dos Direitos do Homem é um requisito da legalidade dos atos da União e que na União não se podem admitir medidas incompatíveis com o respeito desses direitos [62].

170. Por outro lado, decorre da jurisprudência do Tribunal de Justiça que a comunicação de dados pessoais recolhidos de terceiros, públicos ou privados, constitui uma ingerência no direito ao respeito da vida privada, «seja qual for a utilização posterior das informações assim comunicadas» [63]. Além disso, no seu acórdão Digital Rights Ireland e o. [64], o Tribunal de Justiça confirmou que o facto de as autoridades nacionais competentes terem acesso a esses dados constitui uma ingerência suplementar e distinta neste direito fundamental [65]. Além disso, qualquer forma de tratamento dos dados pessoais é visada pelo artigo 8.º da Carta e constitui uma ingerência no direito à proteção desses dados [66]. Por conseguinte, o acesso de que dispõem os serviços de informação americanos aos dados transferidos também é constitutivo de uma ingerência no direito fundamental à proteção dos dados pessoais garantido pelo artigo 8.º da Carta, uma vez que esse acesso constitui um tratamento desses dados.

171. À semelhança do que o Tribunal de Justiça declarou nesse acórdão, a ingerência assim identificada é muito ampla e deve ser considerada particularmente grave, tendo em conta o número importante de utilizadores abrangidos e as quantidades de dados transferidos. Estes factos, associados ao caráter secreto do acesso pelas autoridades americanas aos dados pessoais transferidos para empresas estabelecidas nos Estados Unidos, torna a ingerência extremamente séria.

172. A isto acresce a circunstância de os cidadãos da União, utilizadores do Facebook, não serem informados do facto de o seus dados pessoais estarem de uma forma geral acessíveis para as agências de segurança americanas.

173. Importa também alertar para o facto de o órgão jurisdicional de reenvio ter constatado que, nos Estados Unidos, os cidadãos da União não têm nenhum direito efetivo de serem ouvidos sobre a questão da vigilância e da interceção dos seus dados. O FISC competente exerce uma supervisão, mas o processo da sua competência é secreto e não está sujeito ao contraditório [67]. Considero que se trata de uma ingerência no direito dos cidadãos da União a um recurso efetivo, nos termos do artigo 47.º da Carta.

174. Por conseguinte, está constituída a ingerência que as derrogações aos princípios de «porto seguro» que figuram no anexo I, quarto parágrafo, da Decisão 2000/520, permitem nos direitos fundamentais protegidos pelos artigos 7.°, 8.° e 47.° da Carta.

175. Há, agora, que verificar se essa ingerência é ou não justificada.

62 — V., nomeadamente, acórdão Kadi e Al Barakaat International Foundation/Conselho e Comissão (C-402/05 P e C-415/05 P, EU:C:2008:461, n.º 284 e jurisprudência referida).

63 — Acórdão Österreichischer Rundfunk e o. (C-465/00, C-138/01 e C-139/01, EU:C:2003:294, n.ºs 74 e 75).

64 — C-293/12 e C-594/12, EU:C:2014:238.

65 — N.º 35.

66 — N.º 36.

67 — N.º 7, alínea b), da decisão de reenvio.

176. Em conformidade com o artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos por esta deve ser prevista por lei; e deve respeitar o conteúdo essencial dos seus direitos e liberdades. Na observância do princípio da proporcionalidade, só podem ser introduzidas restrições aos referidos direitos e liberdades 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.

177. Assim, tendo em conta as condições previstas para poder admitir restrições ao exercício dos direitos e liberdades protegidos pala Carta, duvido profundamente que se possa considerar que as restrições em causa no presente processo respeitam o conteúdo essencial dos artigos 7.° e 8.° da Carta. Com efeito, o acesso dos serviços de informação americanos aos dados transferidos parece estender-se ao conteúdo das comunicações eletrónicas, o que viola o conteúdo essencial do direito fundamental ao respeito da vida privada e de outros direitos consagrados no artigo 7.º da Carta. Além disso, na medida em que a formulação ampla das limitações previstas no anexo I, quarto parágrafo, da Decisão 2000/520 permite potencialmente afastar a aplicação do conjunto dos princípios de porto seguro, pode considerar-se que essas limitações afetam o conteúdo essencial do direito fundamental à proteção dos dados pessoais [68].

178. Quanto à questão de saber se a ingerência constatada responde a um objetivo de interesse geral, recordo, antes de mais, que, nos termos do anexo I, quarto parágrafo, alínea b), da Decisão 2000/520, a adesão aos princípios de «porto seguro» é limitada «por legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores avançados por essa autorização».

179. Há que constatar que os «legítimos interesses» a que esta disposição faz referência não estão especificados. Resulta daí uma incerteza quanto ao âmbito de aplicação, potencialmente muitíssimo amplo, dessa derrogação à aplicação dos princípios de «porto seguro» pelas empresas aderentes.

180. A leitura das explicações contidas no título B, do anexo IV, da decisão 2000/520, intitulado «Autorizações legais explícitas», confirma essa impressão, em especial a afirmação de que «[c]laramente, sempre que a legislação norte-americana impõe uma obrigação contraditória, as organizações norte-americanas, aderentes ou não ao 'porto seguro' têm que aplicar a lei». Por outro lado, quanto às autorizações explícitas, é referido que «enquanto os princípios de 'porto seguro' se destinam a colmatar as diferenças entre os regimes europeus e norte-americanos de proteção da vida privada, devemos respeitar as prerrogativas legislativas dos nossos legisladores eleitos».

181. Na minha opinião, decorre daqui que esta derrogação é contrária aos artigos 7.°, 8.° e 52.°, n.º 1, da Carta, na medida em que não prossegue um objetivo de interesse geral definido de maneira suficientemente precisa.

182. Em todo o caso, a facilidade e a generalidade com que a própria Decisão 2000/520, nos seus anexos I, quarto parágrafo, alínea b) e anexo IV B, prevê que esses princípios de porto seguro podem ser afastados por força de normas do direito americano são incompatíveis com a condição de que as derrogações às regras relativas à proteção de dados pessoais devem ser limitadas ao estritamente necessário. É certo que é feita menção à condição de necessidade mas, além de a demonstração dessa condição ser da responsabilidade da empresa em questão, não vejo como é que essa empresa pode subtrair-se a uma obrigação de afastar os princípios de «porto seguro» que emergem de regras de direito que está obrigada a aplicar.

68 — V., a este respeito, acórdão Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238, n.ºs 39 e 40).

183. Consequentemente, é meu entendimento que a Decisão 2000/520 deve ser declarada inválida na medida em que a existência de uma derrogação que permite de uma maneira tão genérica e imprecisa afastar os princípios do sistema «porto seguro» impede ela própria que se considere que esse sistema assegura um nível de proteção adequado aos dados pessoais que são transferidos da União para os Estados Unidos.

184. Agora, no que se refere à primeira categoria de limites previstos no anexo I, quarto parágrafo, alínea a), da Decisão 2000/520 devido a exigências relativas à segurança nacional, de interesse público e de execução legal, só o primeiro objetivo nos parece ser suficientemente preciso para ser considerado um objetivo de interesse geral reconhecido pela União na aceção do artigo 52.º, n.º 1, da Carta.

185. Há que verificar agora a proporcionalidade da ingerência constatada.

186. A este propósito, cabe recordar que «o princípio de proporcionalidade exige, segundo jurisprudência constante do Tribunal de Justiça, que os atos das instituições da União sejam adequados à realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário à realização desses objetivos» [69].

187. Quanto à fiscalização jurisdicional do respeito destes requisitos, «uma vez que estão em causa ingerências em direitos fundamentais, o alcance do poder de apreciação do legislador da União pode revelar-se limitado em função de um certo número de elementos, entre os quais figuram, designadamente, o domínio em questão, a natureza do direito em causa garantido pela Carta, a natureza e a gravidade da ingerência, bem como a sua finalidade» [70].

188. Considero que as decisões que a Comissão adota com fundamento no artigo 25.º, n.º 6, da Diretiva 95/46 estão sujeitas à fiscalização exaustiva do Tribunal de Justiça quanto à proporcionalidade da avaliação efetuada por aquela instituição em relação ao caráter adequado do nível de proteção oferecida por um país terceiro em virtude «da sua legislação interna ou dos seus compromissos internacionais».

189. A este propósito, há que observar que, no seu acórdão Digital Rights Ireland e o. [71], o Tribunal de Justiça declarou que, «tendo em conta, por um lado, o importante papel desempenhado pela proteção dos dados pessoais na perspetiva do direito fundamental ao respeito da vida privada e, por outro, a amplitude e a gravidade da ingerência neste direito que a [d]iretiva [em causa] comporta, o poder de apreciação do legislador da União fica reduzido, havendo que proceder a uma fiscalização estrita» [72].

190. Essa ingerência deve ser apta para realizar o objetivo prosseguido pelo ato da União em causa e ser necessária para atingir esse objetivo.

191. A este respeito, «[q]uanto ao direito ao respeito da vida privada, a proteção deste direito fundamental exige, segundo a jurisprudência constante do Tribunal de Justiça [...], que as derrogações à proteção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário» [73].

192. Na sua fiscalização, o Tribunal de Justiça tem também em conta a circunstância de que «a proteção dos dados pessoais, que resulta da obrigação expressa prevista no artigo 8.º, n.º 1, da Carta, assume particular importância para o direito ao respeito da vida privada consagrado no artigo 7.º desta» [74].

69 — Acórdão Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238, n.º 46 e jurisprudência referida).

70 — *Ibidem*, n.º 47 e jurisprudência referida.

71 — C-293/12 e C-594/12, EU:C:2014:238.

72 — N.º 48.

73 — Acórdão Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238, n.º 52 e jurisprudência referida).

74 — *Ibidem* (n.º 53).

193. Segundo o Tribunal de Justiça que se refere, a este propósito, à jurisprudência do Tribunal Europeu dos Direitos do Homem, «a regulamentação da União em causa deve estabelecer regras claras e precisas que regulem o âmbito e a aplicação da medida em causa e imponham exigências mínimas, de modo a que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos» [75]. O Tribunal de Justiça refere que «[a] necessidade de dispor de tais garantias é ainda mais importante quando [...] os dados pessoais são sujeitos a tratamento automático e existe um risco significativo de acesso ilícito aos mesmos» [76].

194. N minha opinião, existe uma analogia entre o anexo I, quarto parágrafo, alínea a), da Decisão 2000/520 e o artigo 13.º, n.º 1, da Diretiva 95/46. Na primeira disposição, refere-se que a adesão aos princípios de «porto seguro» pode ser limitada pelos «requisitos de segurança nacional, interesse público ou execução legal». Na segunda, prevê-se que os Estados-Membros podem adotar medidas legislativas destinadas a restringir o alcance das obrigações e direitos referidos nos artigos 6.º, n.º 1, 10.º, 11.º, n.º 1, 12.º e 21.º, sempre que tal restrição constitua uma medida necessária à proteção, nomeadamente, da segurança do Estado, da defesa, da segurança pública e da prevenção, investigação, deteção e repressão de infrações penais.

195. Conforme o Tribunal de Justiça salientou no seu acórdão IPI [77], resulta da redação do artigo 13.º, n.º 1, da Diretiva 95/46 que os Estados-Membros só podem prever as medidas visadas nesta disposição quando estas sejam necessárias. A natureza «necessária» das medidas condiciona assim a faculdade que a referida disposição confere aos Estados-Membros [78]. Para o tratamento de dados pessoais na União, os limites previstos no artigo 13.º desta diretiva devem ser considerados circunscritos ao estritamente necessário para alcançar o objetivo prosseguido. Na minha opinião, deve aplicar-se o mesmo em relação aos limites aos princípios de «porto seguro» que estão previstos no anexo I, quarto parágrafo, da Decisão 2000/520.

196. Ora, há que constatar que nem todas as versões linguísticas fazem menção ao critério de necessidade na redação do anexo I, quarto parágrafo, alínea a), da Decisão 2000/520. É assim o caso, nomeadamente, da versão em língua francesa que refere que «[a] adesão a estes princípios pode ser limitada [...] para observar requisitos de segurança nacional, interesse público ou execução legal», ao passo que, a título de exemplo, as versões linguísticas espanhola, alemã e inglesa referem que as limitações introduzidas devem ser necessárias para alcançar os objetivos *supra* mencionados.

197. Seja como for, os elementos factuais que são avançados pelo órgão jurisdicional de reenvio e pela Comissão nas suas comunicações *supra* mencionadas mostram claramente que, na prática, a aplicação dessas limitações não está circunscrita ao estritamente necessário para alcançar os objetivos visados.

198. Observo, a este propósito, que o acesso aos dados pessoais transferidos de que dispõem os serviços de informação americanos abrange de maneira generalizada todas as pessoas, todos os meios de comunicação eletrónica e todos os dados transferidos, incluindo o conteúdo das comunicações, sem que seja feita qualquer diferenciação, limitação ou exceção em função do objetivo geral prosseguido [79].

199. Com efeito, o acesso dos serviços de informação americanos aos dados transferidos diz respeito de maneira global às pessoas que utilizam serviços de comunicações eletrónicas sem que se exija que as pessoas em causa constituam uma ameaça para a segurança nacional [80].

75 — *Ibidem* (n.º 54 e jurisprudência referida).

76 — *Ibidem* (n.º 55 e jurisprudência referida).

77 — C-473/12, EU:C:2013:715.

78 — N.º 32.

79 — V., por analogia, acórdão Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238, n.º 57 e jurisprudência referida).

80 — *Ibidem* (n.ºs 58 e 59).

200. Uma tal vigilância em larga escala e não dirigida é desproporcionada por natureza e constitui uma ingerência injustificada nos direitos garantidos pelos artigos 7.° e 8.° da Carta.

201. Conforme o Parlamento salientou, com razão, nas suas observações, uma vez que é impossível ao legislador da União ou dos Estados-Membros adotar disposições legislativas que, em violação da Carta, prevejam uma vigilância em larga escala e não dirigida, decorre daí, necessariamente, que, *a fortiori*, não se pode considerar que países terceiros asseguram um nível de proteção adequado dos dados pessoais dos cidadãos da União quando a sua regulamentação autoriza efetivamente a vigilância e a interceção em larga escala e não dirigida deste tipo de dados.

202. Além disso, importa sublinhar que o sistema porto seguro conforme definido pela Decisão 2000/520 não contem as garantias adequadas para evitar um acesso em larga escala e generalizado aos dados transferidos.

203. A este respeito, observo que o Tribunal de Justiça destacou no seu acórdão Digital Rights Ireland e o.[81] a importância de estabelecer «regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta»[82]. Essa ingerência deve ser, segundo o Tribunal de Justiça, «enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário»[83]. O Tribunal de Justiça também salientou, nesse acórdão, a necessidade de prever «garantias suficientes, como exige o artigo 8.º da Carta, que permitam assegurar uma proteção eficaz dos dados [pessoais] conservados contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos»[84].

204. Ora, há que declarar que os mecanismos de arbitragem privada e a FTC, por causa do seu papel limitado aos conflitos de natureza comercial, não constituem meios para contestar o acesso dos serviços de informação americanos aos dados pessoais transferidos da União.

205. A competência da FTC abarca as práticas e os atos desleais ou desonestos praticados no comércio ou que nele se refletem, e não se estende então à recolha e ao uso de informação pessoal para fins não comerciais[85]. O domínio de jurisdição limitada da FTC restringe o direito dos particulares à proteção dos seus dados pessoais. A FTC não foi criada para assegurar, como é o caso na União das autoridades nacionais de controlo, a proteção do direito individual à vida privada, mas para garantir um comércio leal e fiável para os consumidores, o que limita, de facto, as suas capacidades de intervenção no domínio relativo à proteção de dados pessoais. Por conseguinte, a FTC não desempenha um papel comparável ao das autoridades nacionais de controlo previstas no artigo 28.º da Diretiva 95/46.

206. Os cidadãos da União cujos dados foram transferidos podem dirigir-se a organismos de arbitragem especializados estabelecidos nos Estados Unidos como o TRUSTe e o BBBOnline para pedir esclarecimentos sobre a questão de saber se a empresa que tem os seus dados pessoais viola as condições do regime de autocertificação. A arbitragem privada assegurada por organismos como o TRUSTe não pode tratar as violações do direito à proteção de dados pessoais que são cometidos por organismos ou autoridades diferentes das empresas autocertificadas. Estes organismos de arbitragem não têm qualquer competência para decidir sobre a legalidade das atividades das agências de segurança americanas.

81 — C-293/12 e C-594/12, EU:C:2014:238.

82 — *Ibidem* (n.º 65).

83 — *Idem.*

84 — *Ibidem* (n.º 66).

85 — V., a este respeito, anexo II, FAQ 11, da Decisão 2000/520, sob «Atividade da FTC», e seus anexos III, V e VII.

207. Consequentemente, nem a FTC nem os organismos privados de arbitragem têm competência para controlar as possíveis violações dos princípios de proteção de dados pessoais cometidas por autores públicos, como as agências de segurança americanas. No entanto, essa competência é essencial para garantir plenamente o direito à proteção efetiva desses dados. Por conseguinte, a Comissão, ao adotar e manter em vigor a Decisão 2000/520, que não podia constatar que havia, relativamente a todos os dados pessoais transferidos para os Estados Unidos, uma proteção adequada do direito conferido pelo artigo 8.º, n.º 3, da Carta, isto é que uma autoridade independente exerceria uma fiscalização efetiva do respeito dos requisitos de proteção e segurança desses dados.

208. Por conseguinte, há que constatar a falta, no sistema «porto seguro» previsto na Decisão 2000/520, de uma autoridade independente que pudesse fiscalizar que a aplicação das derrogações aos princípios de «porto seguro» está limitada ao estritamente necessário. Ora, vimos que semelhante fiscalização, efetuada por uma autoridade independente constitui, com base no direito da União, um elemento essencial do respeito da proteção das pessoas relativamente ao tratamento dos dados pessoais [86].

209. A este respeito, importa sublinhar o papel que, no sistema de proteção de dados pessoais em vigor na União, as autoridades nacionais de controlo desempenham na fiscalização das limitações previstas no artigo 13.º da Diretiva 95/46. Nos termos do artigo 28.º, n.º 4, segundo parágrafo, desta diretiva «[q]ualquer pessoa pode apresentar à autoridade de controlo um pedido de verificação da licitude de qualquer tratamento de dados, sempre que sejam aplicáveis as disposições nacionais adotadas por força do artigo 13.º». Por analogia, considero que a menção dos limites à aplicação dos princípios de «porto seguro» ao anexo I, quarto parágrafo, da Decisão 2000/520 devia ter sido acompanhada da implementação de um mecanismo de fiscalização assegurado por uma autoridade independente especializada no domínio da proteção de dados pessoais.

210. A intervenção das autoridades de controlo independentes está, com efeito, no cerne do sistema europeu de proteção de dados pessoais. Por conseguinte, foi com naturalidade que a existência dessas autoridades foi considerada, desde logo, como um dos requisitos necessários à constatação do nível de proteção oferecida pelos países terceiros. Trata-se aí de um requisito para que o fluxo de dados a partir do território dos Estados-Membros para o de países terceiros não seja proibido em conformidade com o artigo 25.º da Diretiva 95/46 [87]. Como refere o documento de discussão adotado pelo grupo de trabalho instituído pelo artigo 29.º desta diretiva, na Europa, existe um consenso generalizado de que «um sistema de 'fiscalização externa' sob forma de uma autoridade independente, constitui um elemento necessário de qualquer sistema destinado a assegurar a observância das regras em matéria de proteção dos dados» [88].

211. Além disso, recordo que o FISC não oferece um recurso jurisdicional efetivo aos cidadãos da União cujos dados pessoais são transferidos para os Estados Unidos. Com efeito, as proteções contra a vigilância pelos serviços governamentais no âmbito da section 702 da Lei de 1978 relativa à vigilância dos serviços de informação estrangeiros só se aplicam aos cidadãos americanos e aos cidadãos estrangeiros que residam legal e permanentemente nos Estados Unidos. Como a própria Comissão salientou, a fiscalização dos programas de recolha de informações poderia ser melhorado mediante o reforço do papel do FISC e a introdução da possibilidade de os particulares interporem recursos. Esses mecanismos poderiam reduzir o tratamento de dados pessoais dos cidadãos da União que não sejam pertinentes para efeitos de segurança nacional [89].

86 — V. acórdão Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238, n.º 68 e jurisprudência referida).

87 — V. Poullet, Y., «L'autorité de contrôle: 'vues' de Bruxelles», *Revue française d'administration publique*, n.º 89, janeiro-março 1999, p. 69, especialmente p. 71.

88 — V. p. 7 do documento de trabalho WP 12 da Comissão, mencionado na nota 56 de pé de página.

89 — Pp. 10 e 11 da comunicação da Comissão referido na nota 2.

212. Por outro lado, a própria Comissão referiu que os cidadãos da União não têm qualquer possibilidade de obterem acesso ou solicitarem a retificação ou a supressão dos dados, ou apresentarem um recurso administrativo ou judicial caso, no âmbito de programas de vigilância americanos, os seus dados pessoais sejam recolhidos e tratados posteriormente [90].

213. Por último, há que referir que as normas americanas relativas à proteção da vida privada podem ser objeto de uma aplicação diferenciada entre os cidadãos americanos e os cidadãos estrangeiros [91].

214. Resulta do que precede que a Diretiva 2000/520 não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta. Por conseguinte, há que concluir que esta decisão e a sua aplicação comportam uma ingerência de grande amplitude e de particular gravidade nestes direitos fundamentais, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário.

215. Por conseguinte, ao adotar e manter em vigor a Decisão 2000/520, a Comissão excedeu os limites que o respeito do princípio da proporcionalidade impõe à luz dos artigos 7.°, 8.° e 52.°, n.º 1 da Carta. A isto acresce a constatação de uma ingerência não justificada no direito dos cidadãos da União a um recurso jurisdicional efetivo, protegido pelo artigo 47.º da Carta.

216. Consequentemente, esta decisão deve ser declarada inválida na medida em que, em virtude das violações dos direitos fundamentais precedentemente descritas, não se pode considerar que o sistema «porto seguro» que esta instaura, assegura um nível de proteção adequado aos dados pessoais que são transferidos da União no âmbito desse sistema.

217. Perante esta constatação de violação dos direitos fundamentais dos cidadãos da União, considero que a Comissão devia ter suspendido a aplicação da Decisão 2000/520.

218. Esta decisão vigora por prazo indeterminado. Ora, o presente processo demonstra que o caráter adequado do nível de proteção oferecido por um país terceiro pode evoluir com o tempo em função da alteração das circunstâncias simultaneamente factuais e jurídicas que fundamentaram a referida decisão.

219. Saliento que a própria Decisão 2000/520 contém disposições que preveem a possibilidade de a Comissão a adaptar em função das circunstâncias.

220. Assim, resulta do considerando 9 desta decisão que «[o] 'porto seguro' criado pelos princípios e pelas FAQ pode necessitar de revisão à luz da experiência dos desenvolvimentos relativos à proteção da vida privada em circunstâncias em que a tecnologia torna cada vez mais fáceis a transferência e o tratamento de dados pessoais e à luz de relatórios relativos à aplicação dada pelas entidades responsáveis».

221. Do mesmo modo, nos termos do artigo 3.º, n.º 4, da referida decisão, «[s]e a informação recolhida nos termos dos n.ºs 1 a 3 demonstrar que os organismos responsáveis pelo cumprimento dos princípios em conformidade com as FAQ nos Estados Unidos da América não desempenham eficazmente as suas funções, a Comissão deve informar o Department of Commerce norte-americano e, se necessário, apresentar um projeto de medidas [...] para revogar ou suspender a presente decisão ou limitar o seu âmbito».

90 — P. 7.2, p. 20, da comunicação referida na nota 58.

91 — V., sobre esta questão, Kuner, C., «Foreign Nationals and Data Protection Law: A Transatlantic Analysis», *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, p. 213, especialmente pp. 216 e segs.

222. Além disso, segundo o artigo 4.º, n.º 1, da Decisão 2000/520, esta «pode ser adaptada em qualquer altura, à luz da experiência proporcionada pela sua aplicação e/ou se o nível de proteção proporcionado pelos princípios e pelas FAQ for considerado insuficiente pela lei norte-americana. Em qualquer caso, a Comissão deve avaliar a aplicação da presente decisão com base na informação disponível, três anos após a sua notificação aos Estados-Membros, e informar o comité estabelecido pelo artigo 31.º da Diretiva 95/46[…] de todas as conclusões pertinentes e, nomeadamente, de todas as provas que possam afetar a apreciação da adequação do nível de proteção do disposto no artigo 1.º da presente decisão, nos termos do artigo 25.º da diretiva [95/46]». Nos termos do artigo 4.º, n.º 2, da Decisão 2000/520, «[a] Comissão apresentará, se necessário, projetos de medidas de acordo com o previsto no artigo 31.º da diretiva».

223. A Comissão concluiu nas suas observações que «existe uma forte probabilidade de que a adesão aos princípios de «porto seguro» esteja limitada de uma maneira que já não responde às condições estritamente circunscritas da isenção prevista em matéria de segurança nacional» [92]. A este respeito, observa que «[a]s revelações em questão mostram um grau de vigilância indiferenciada em grande escala que não é compatível com o critério de necessidade previsto nesta isenção nem, de maneira mais geral, com o direito à proteção dos dados pessoais consagrada no artigo 8.º da Carta» [93]. Por outro lado, a própria Comissão constatou que «[o] alcance [dos] programas de vigilância, juntamente com a desigualdade de tratamento dos cidadãos da [União], compromete o grau de proteção conferido pelo acordo «porto seguro» [94].

224. Além disso, a Comissão reconheceu expressamente, na audiência, que, no âmbito da Decisão 2000/520, tal como é aplicada atualmente, não há garantia de que o direito dos cidadãos da União à proteção dos seus dados seja assegurada. No entanto, segundo a Comissão, esta conclusão não é suscetível de tornar inválida esta decisão. Embora a Comissão concorde com a afirmação de que deve agir perante novas circunstâncias, considera que tomou as medidas adequadas e proporcionadas ao encetar negociações com os Estados Unidos para reformar o sistema «porto seguro».

225. Discordo. Com efeito, no entretanto, as transferências de dados pessoais para os Estados Unidos devem poder ser suspensas por iniciativa das autoridades nacionais de controlo ou na sequência de queixas que lhes sejam apresentadas.

226. Por outro lado, considero que, face a essas constatações, a Comissão devia ter suspendido a aplicação da Decisão 2000/520. Com efeito, o objetivo da proteção dos dados pessoais prosseguido pela Diretiva 95/46 e pelo artigo 8.º da Carta impõe obrigações não só aos Estados-Membros, mas também às instituições da União, como resulta do artigo 51.º, n.º 1, da Carta.

227. Na sua avaliação do nível de proteção assegurado por um país terceiro, a Comissão deve analisar não só a legislação interna e os compromissos internacionais desse país, terceiro, mas também a maneira como a proteção dos dados pessoais é assegurada na prática. Se a análise da prática revelar disfunções, a Comissão deve reagir e, se for caso disso, suspender e/ou adaptar sem demora a sua decisão.

228. Como vimos nos desenvolvimentos precedentes, a obrigação que recai sobre os Estados-Membros consiste principalmente em assegurar, pela ação das respetivas autoridades nacionais de controlo, o respeito das regras previstas pela Diretiva 95/46.

92 — N.º 44.

93 — *Idem.*

94 — P. 5 da comunicação da Comissão referida na nota 2.

229. A Comissão tem a obrigação de suspender a aplicação de uma decisão que adotou com fundamento no artigo 25.º, n.º 6, dessa diretiva no caso de incumprimentos comprovados por parte do país terceiro em causa e durante as negociações encetadas com esse país terceiro para pôr termo a esses incumprimentos.

230. Recordo que uma decisão adotada pela Comissão com fundamento nesta disposição tem por objeto constatar que um país terceiro «assegura» um nível de proteção adequado aos dados pessoais objeto de uma transferência para um país terceiro. O vocábulo «assegura», conjugado no presente, implica que, para poder ser mantida, essa decisão deve dizer respeito a um país que continua, depois da aprovação da referida decisão, a garantir esse nível de proteção adequado.

231. Segundo o considerando 57 da Diretiva 95/46, «sempre que um país terceiro não ofereça um nível de proteção adequado, a transferência de dados pessoais para esse país deve ser proibida».

232. Nos termos do artigo 25.º, n.º 4, desta diretiva, «[s]empre que a Comissão verificar, nos termos do procedimento previsto no n.º 2 do artigo 31.º, que um país terceiro não assegura um nível de proteção adequado na aceção do n.º 2 do presente artigo, os Estados-Membros tomarão as medidas necessárias para impedir qualquer transferência de dados de natureza idêntica para o país terceiro em causa». Por outro lado, o artigo 25.º, n.º 5, da referida diretiva dispõe que «[e]m momento oportuno, a Comissão encetará negociações com vista a obviar à situação resultante da constatação feita em aplicação do n.º 4».

233. Resulta desta última disposição que, no sistema implementado pelo artigo 25.º da Diretiva 95/96, as negociações encetadas com um país terceiro têm por objetivo corrigir uma falta de nível de proteção adequado constatada em conformidade com o procedimento previsto no artigo 31.º, n.º 2, desta diretiva. No caso em apreço, a Comissão não constatou formalmente, em conformidade com esse procedimento, que o sistema «porto seguro» já não assegurava um nível de proteção adequado. Assim sendo, se a Comissão decidiu iniciar negociações com os Estados Unidos, é porque, previamente, considerou que o nível de proteção assegurado por esse país terceiro já não era adequado.

234. Embora tivesse conhecimento de disfunções na aplicação da Decisão 2000/520, a Comissão não suspendeu nem adaptou a referida decisão arrastando assim o prosseguimento da violação dos direitos fundamentais das pessoas cujos dados pessoais continuaram e continuam a ser transferidos no âmbito do sistema «porto seguro».

235. Ora, o Tribunal de Justiça já declarou, é certo que noutro contexto, que cabe à Comissão zelar por uma adaptação da regulamentação aos novos dados [95].

236. Essa omissão de agir da Comissão, que viola diretamente os direitos fundamentais protegidos pelos artigos 7.°, 8.° e 47.° da Carta, constitui, na minha opinião, um motivo suplementar para declarar inválida a Decisão 2000/520 no âmbito do presente pedido de decisão prejudicial [96].

95 — V., neste sentido, acórdão Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, n.º 40).

96 — Embora o Tribunal de Justiça tenha declarado no seu acórdão T. Port (C-68/95, EU:C:1996:452), que «o Tratado não previu a possibilidade de um reenvio pelo qual um órgão jurisdicional nacional solicitasse ao Tribunal de Justiça a declaração a título prejudicial da omissão de uma instituição» (n.º 53), parece que adotou uma posição mais favorável a essa possibilidade no seu acórdão Ten Kate Holding Musselkanaal e o. (C-511/03, EU:C:2005:625, n.º 29).

III – **Conclusão**

237. Tendo em consideração os desenvolvimentos que antecedem, proponho que o Tribunal de Justiça responda às questões submetidas pela High Court nos seguintes termos:

O artigo 28.° 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, lido à luz dos artigos 7.° e 8.° da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que a existência de uma decisão adotada pela Comissão Europeia com fundamento no artigo 25.°, n.° 6, da Diretiva 95/46, não impede que uma autoridade nacional de controlo investigue uma queixa que denuncia que um país terceiro não assegura um nível de proteção adequado aos dados pessoais transferidos e, se for caso disso, suspenda a transferência desses dados.

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